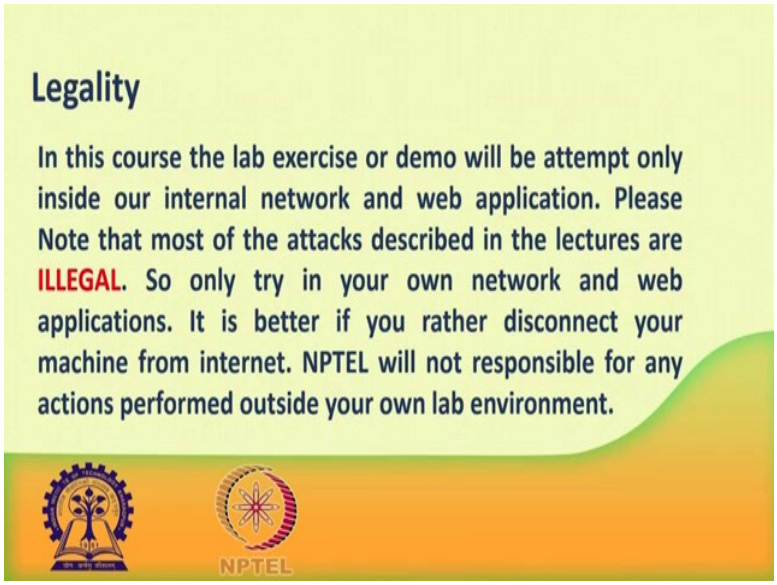
Ethical Hacking
Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 17
Demonstration Part II

(Refer Slide Time: 00:18)



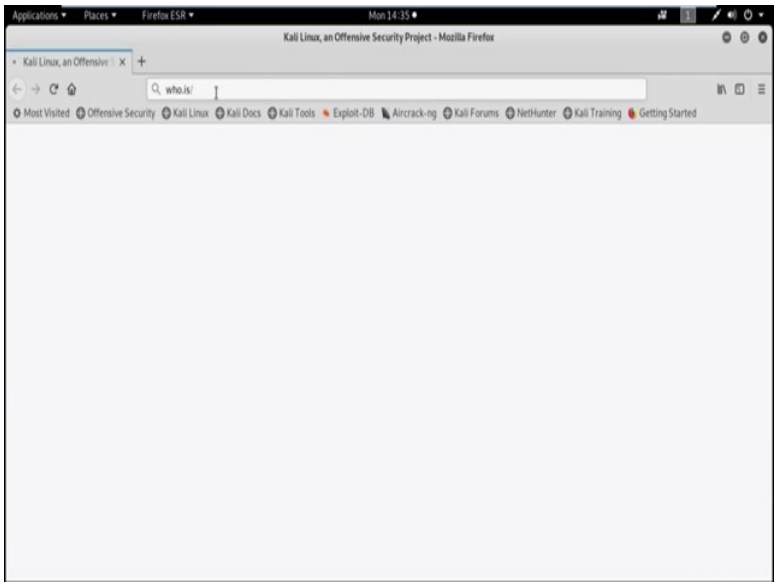
In this course the lab exercise or demo will be attempt only inside our internal network and web application. Please note that most of the attacks described in the lectures are illegal. So, only try your own network and web application. It is better if you would rather disconnect your machine from internet. NPTEL will not be responsible for any action performed outside your own lab environment.

(Refer Slide Time: 00:54)

Now, we will discuss about first phase of hacking reconnaissance. Reconnaissance is the phase where the attacker gathers information about the target using the active path, passive needs, passive information gathered. In passive information gathering, we gather a information not find directly communicating with effective. We may gather information from any other source, may from search, different search engines, social site or company website.

We can also gather information using open web like who is Netcraft history of the website like archive.org, maybe sometimes we also use Google search and some search operator in Google like site in url, file type etc.

(Refer Slide Time: 01:59)

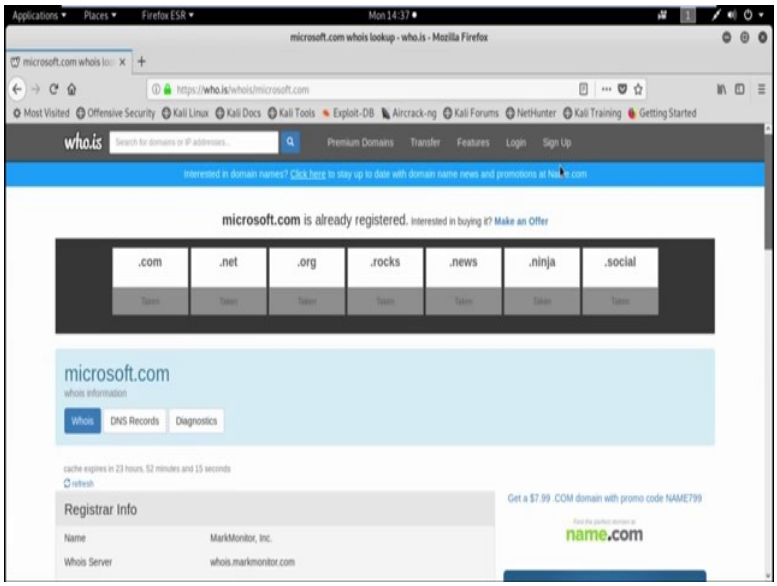


Now have a look WHOIS database looker. WHOIS allows us to access information about the target including registration details, IP address, contact information containing the addresses, email id, phone number. It also displays domain owner and domain register.

(Refer Slide Time: 02:40)

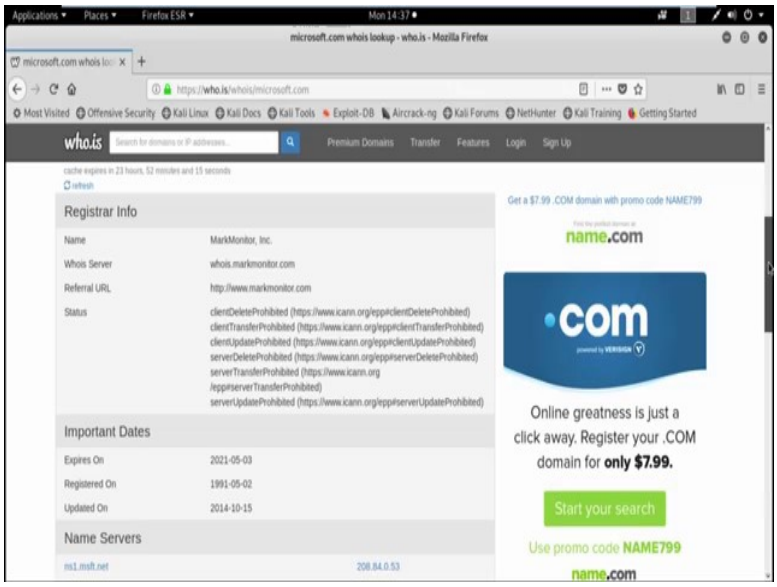
Suppose we want to gather information about the domain $microsoft.com$.

(Refer Slide Time: 03:01)



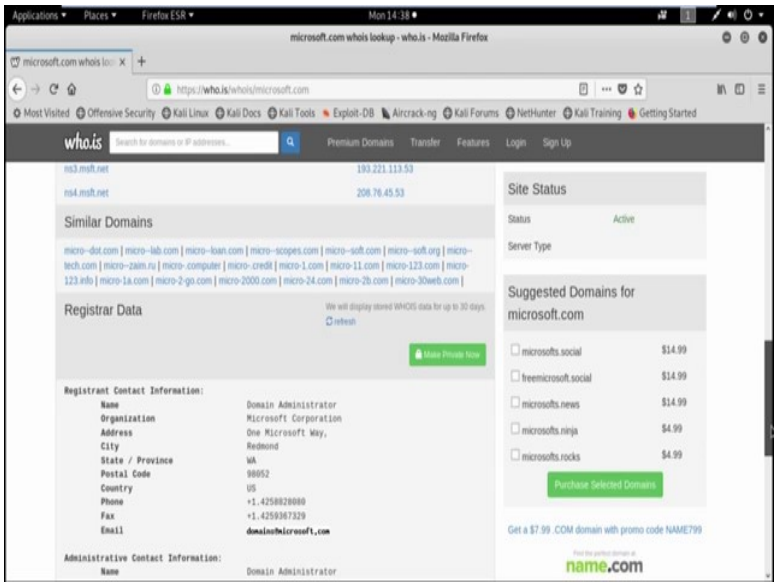
Now, see the result.

(Refer Slide Time: 03:08)



We already gather information about the registered date, update on, expire on and different name server.

(Refer Slide Time: 03:21)

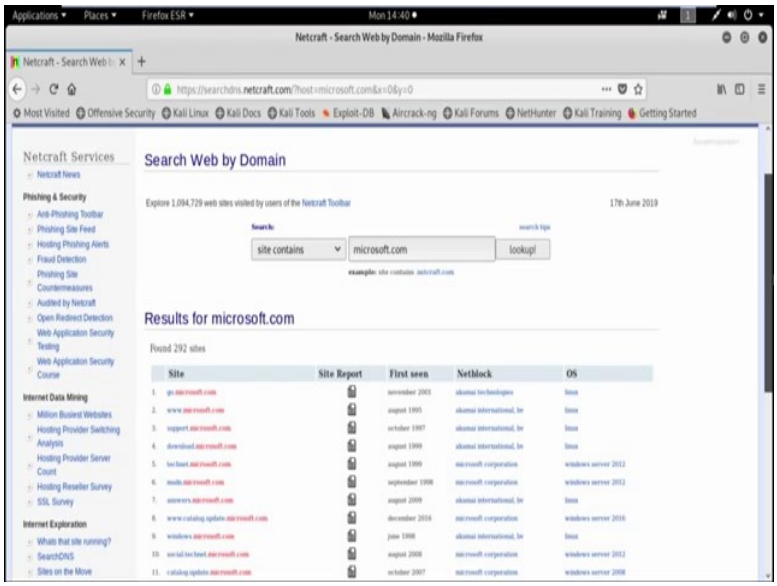


Registered data like name, organization, address, city, state, postal code country even if email id and phone number also.

(Refer Slide Time: 03:38)

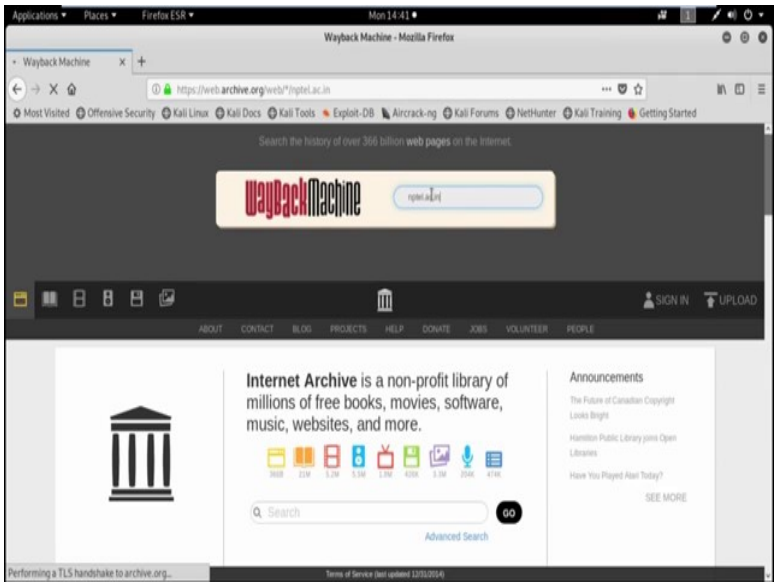
Now, using Netcraft we can also gather information. Netcraft is an internet service company based in England. Using this service one can find the list of sub domain and the operating system of the corresponding server. Now suppose using Netcraft tool we are going to gather information about the same domain $microsoft.com$.

(Refer Slide Time: 04:21)



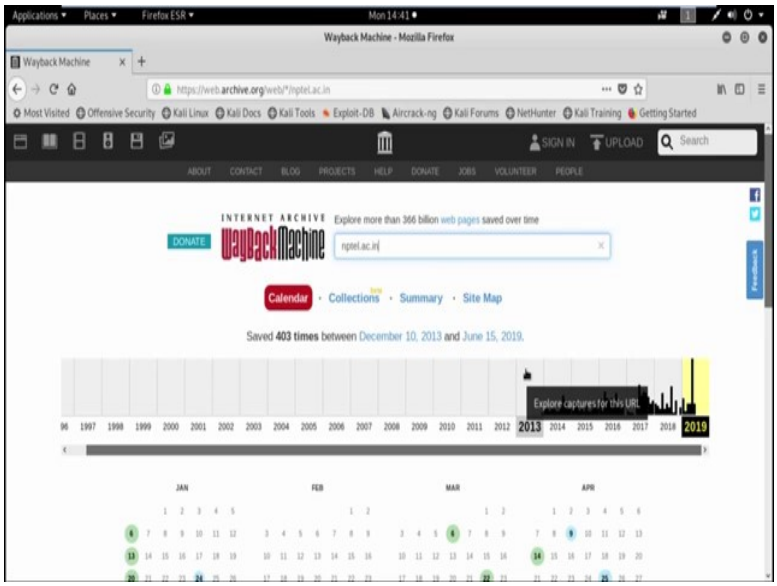
Now, see we get all the sub domain for that particular domain $microsoft.com$ and the corresponding OS in which that particular server is running.

(Refer Slide Time: 04:37)



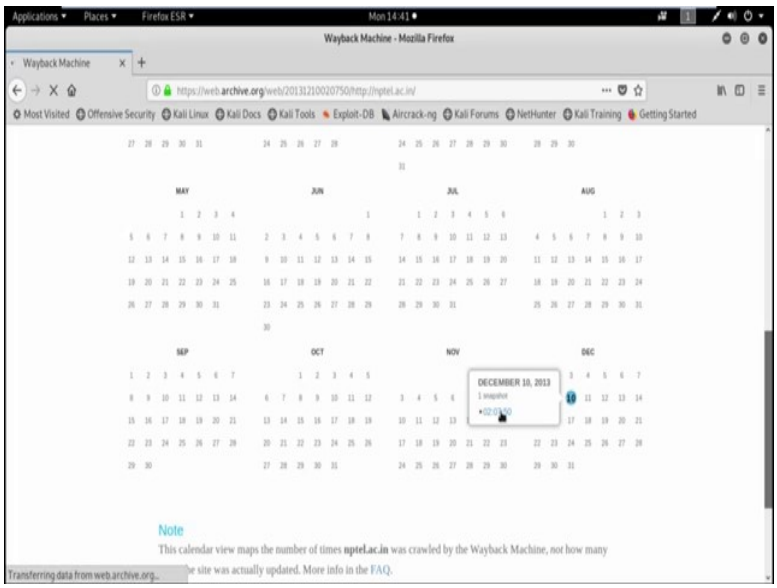
History of the website; it is very easy to get a complete history of any website using $www.archive.org$. Now suppose using the archive dot org we are going to search the history of the website $nptel.ac.in$.

(Refer Slide Time: 05:29)



Now, see the particular domain started in the year 2013 and year 2013 there is only one update that is on December 10.

(Refer Slide Time: 05:42)



(Refer Slide Time: 05:51)

Now, suppose I want to see the website at that particular date 10th December 2013. It is just welcome to. Now suppose I want to see the web application in any other previous date.

(Refer Slide Time: 06:20)

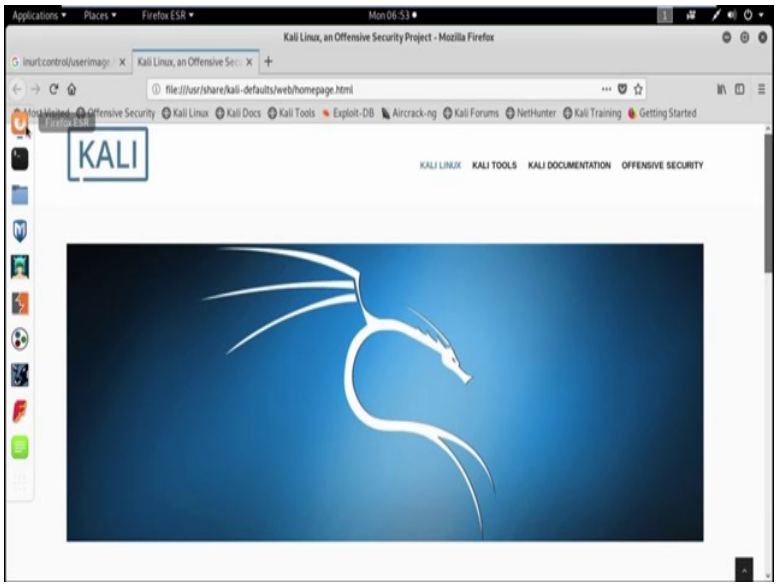
Now, see the website is look like this in December 28, 2014. So, now this way we can gather information from a web application in any previous day. Google search; the Google search engine is a hacker's best friend especially when it comes to information gathering. Google supports the use of various search operators which allow user to

narrow down and pinpoint search results. Now, we discuss about some basic operators in Google search.

(Refer Slide Time: 07:09)

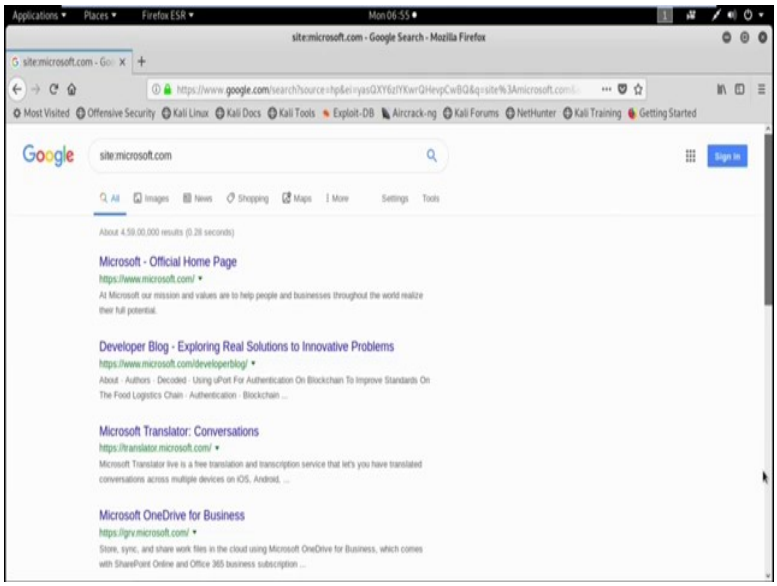
Site operator; site operator has been used to limit the result for a particular site. For example, suppose we are going to limit our search result with only the site $microsoft.com$. So, now I am opening my browser and using the site operator.

(Refer Slide Time: 07:37)



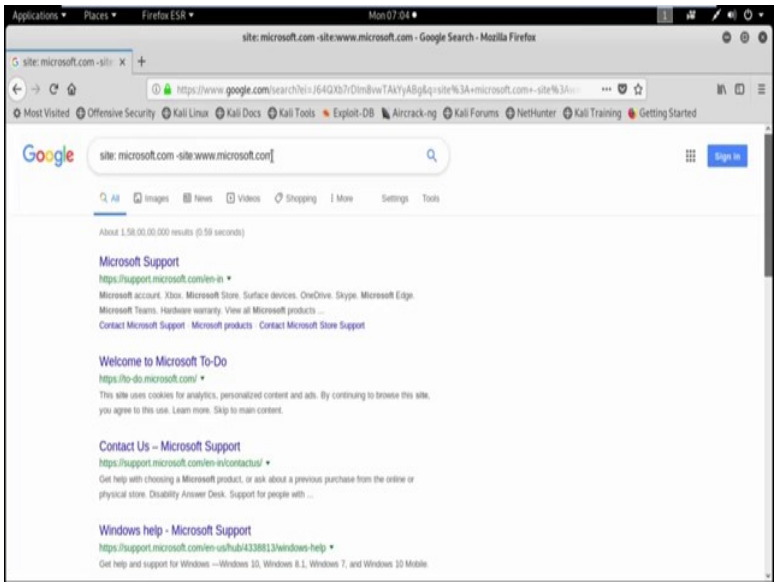
I will search for only $microsoft.com$ domain.

(Refer Slide Time: 08:01)



Now, see the result. We get only those result which is related with the site $microsoft.com$. See $microsoft.com$, $microsoft.com$. So, all the search result is basically related with the domain that means with the site $microsoft.com$. Let us filter those out to see what others sub domains may exist at $microsoft.com$.

(Refer Slide Time: 08:49)

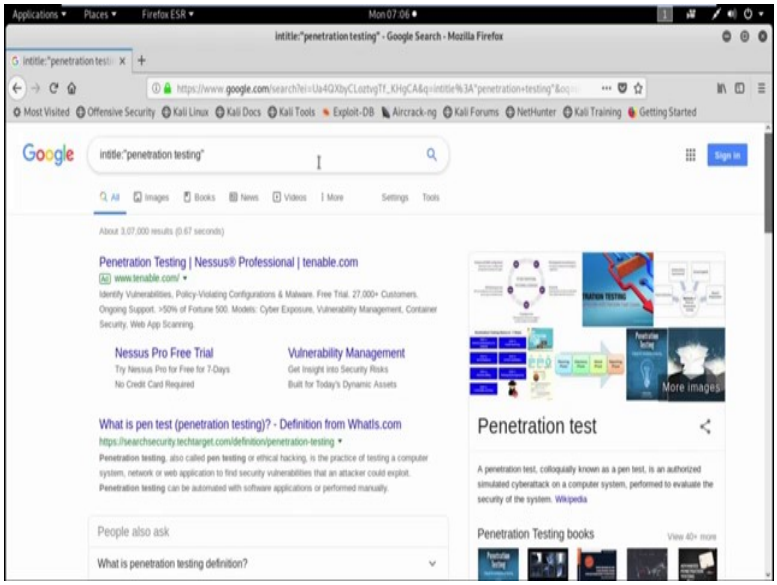


So, we are going to search site $microsoft.com - www.microsoft.com$. So, now see this result basically subtract all the result which is related with the sub domain $www.microsoft.com$. So, you got all the results with the site $microsoft.com$ other

than the sub domain $www.microsoft.com$. So, see we can get $support.microsoft.com$, $todo.microsoft.com$, $support.microsoft.com$ and so on.

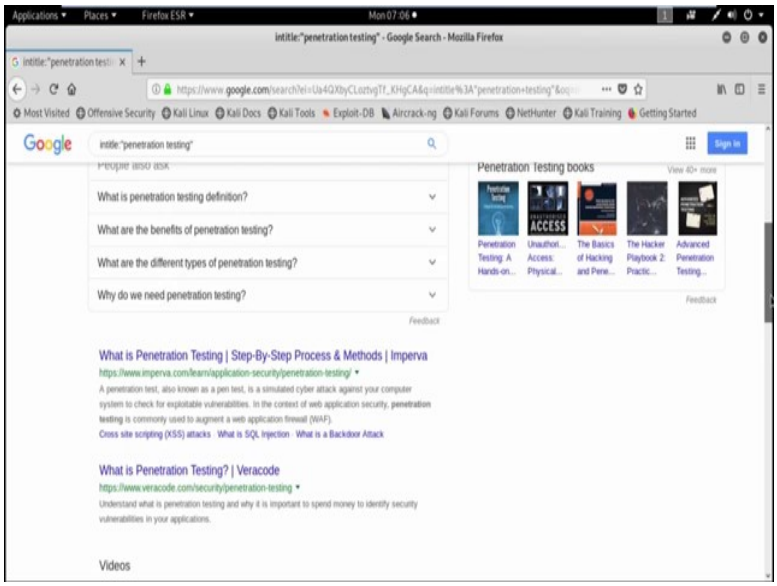
Now, we can also use intitle search parameter. So, using intitle search parameters, search only in those page title for a word or phrase, use exact match for pages. So, for example suppose I am searching intitle.

(Refer Slide Time: 10:06)



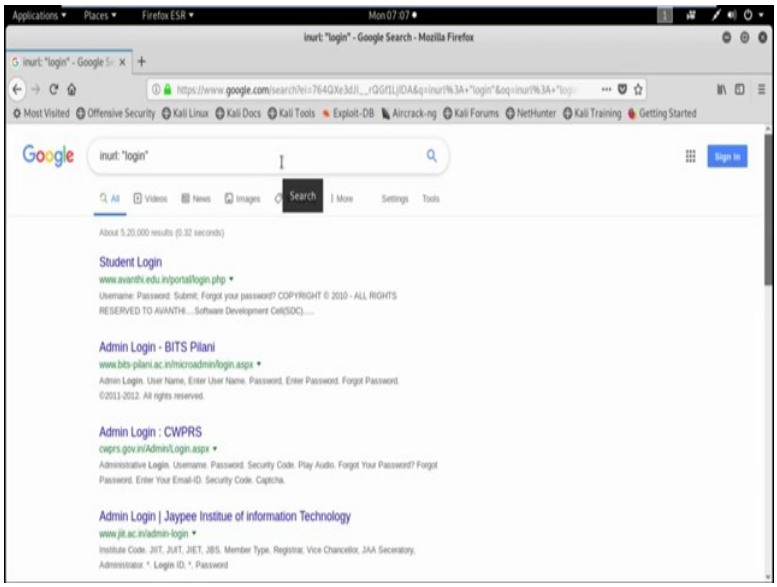
Then with the phrase penetration testing, so we will get all the result where penetration term or penetration testing phrase is basically related. See penetration testing here is also the term penetration testing is there.

(Refer Slide Time: 10:49)



So, by using intitle search parameter we can search a particular word phrase. Now, we also used inurl search parameter. So, using inurl search parameter we are basically look for a word or phrase in the document url that can combine with other terms.

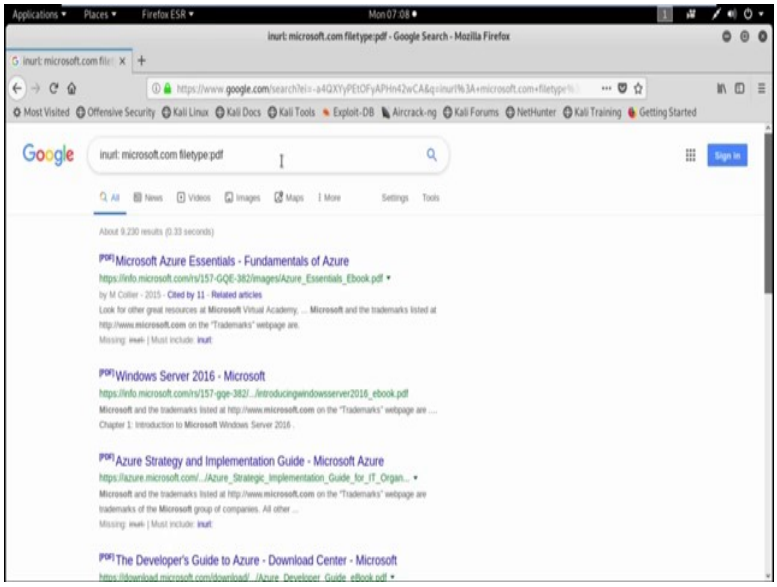
(Refer Slide Time: 11:19)



Inurl colon then suppose I am searching login term. See so, using inurl search parameter we search all the login pages. That means, where the login page is available, it basically search that particular inurl.

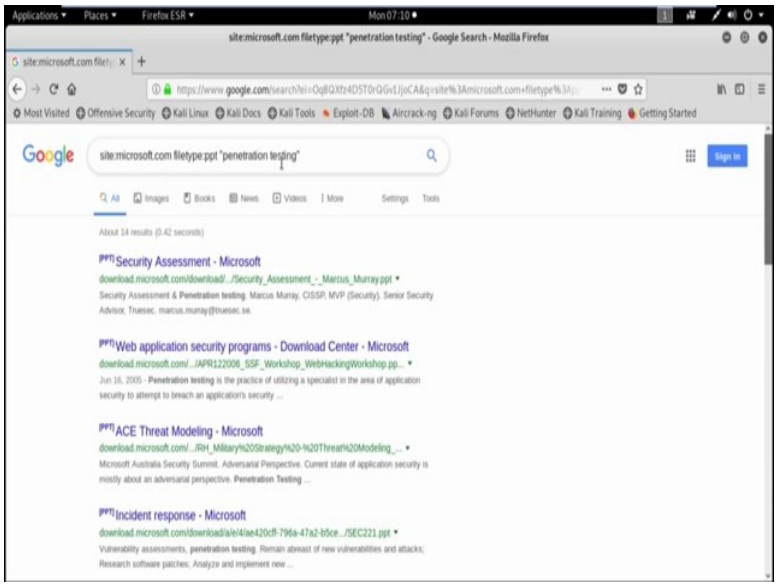
Now, using the search parameter file type we can also search a particular file type like pdf, doc, excel, ppt like this. So, it basically match only a specific file type.

(Refer Slide Time: 12:12)



For example suppose inurl then $microsoft.com$ and file type is basically pdf. Now see in the url $microsoft.com$ we search for the file type pdf. So, for this particular search operation we get all the pdf file type in the url $microsoft.com$. Here we can also combine two or more search operator to narrow down our search result. In site $microsoft.com$ we want to find ppt file with specific phrase penetration testing. So, our search string is like this.

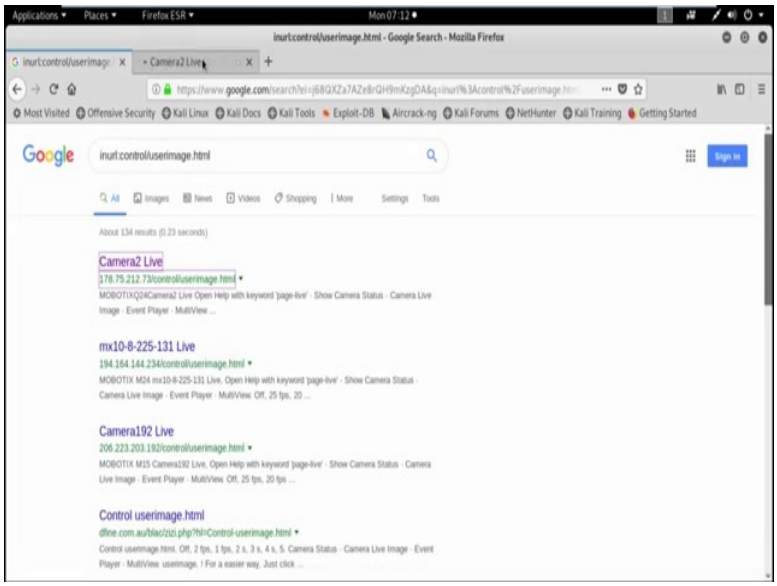
(Refer Slide Time: 13:27)



Site then $microsoft.com$, then file type ppt and then the term penetration testing. Now see we get all the ppt file for a particular site $microsoft.com$ related with the term penetration testing. Now how to use these search parameter to exploit some domain or IP addresses. I am giving you one example. Most of the CCTV camera application use the page with default name $control/userimage.html$.

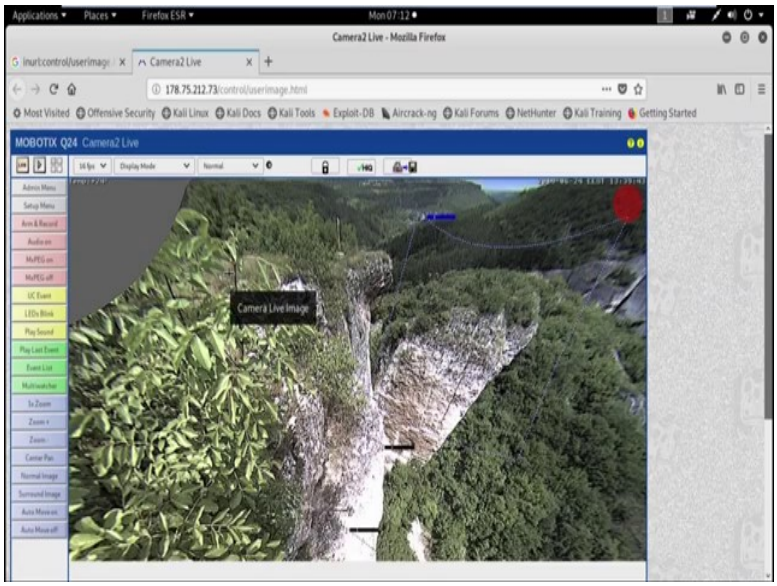
So, use the search parameter inurl $control/userimage.html$ to find out all the CCTV camera facing to the internet with default page $control/userimage.html$. Now have a look.

(Refer Slide Time: 15:01)



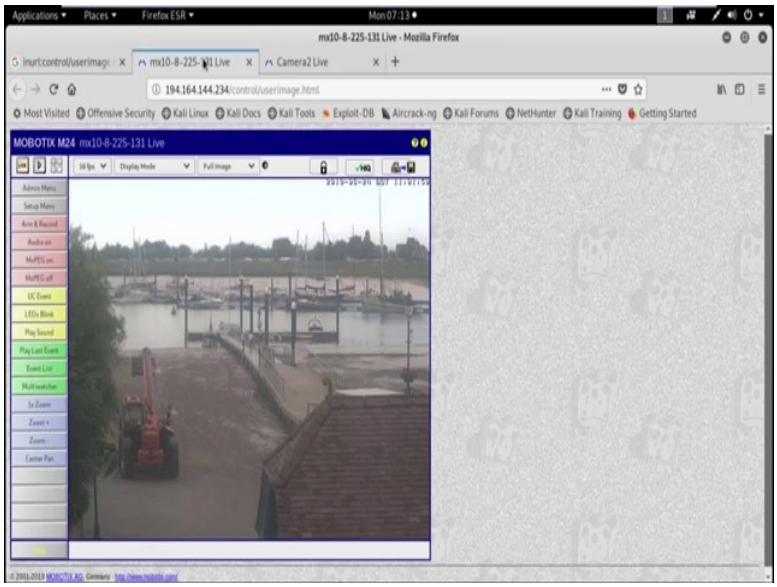
Inurl: *control*/*userimage*. *html*. Now see we got lots of CCTV camera IP address which is facing to the internet. Now some of the CCTV camera are vulnerable. They may do not have any user id or password. Sometimes they only use the default user id or password. Other than these we can also perform maybe brute force attack, maybe dictionary attack for penetrating inside the CCTV camera. Now suppose I am opening the first link, now see wow.

(Refer Slide Time: 16:07)



It is a live camera. There is no user id or password. So, this camera is not secure and it is facing to the internet. So, we get all the video which basically captured using this particular CCTV camera.

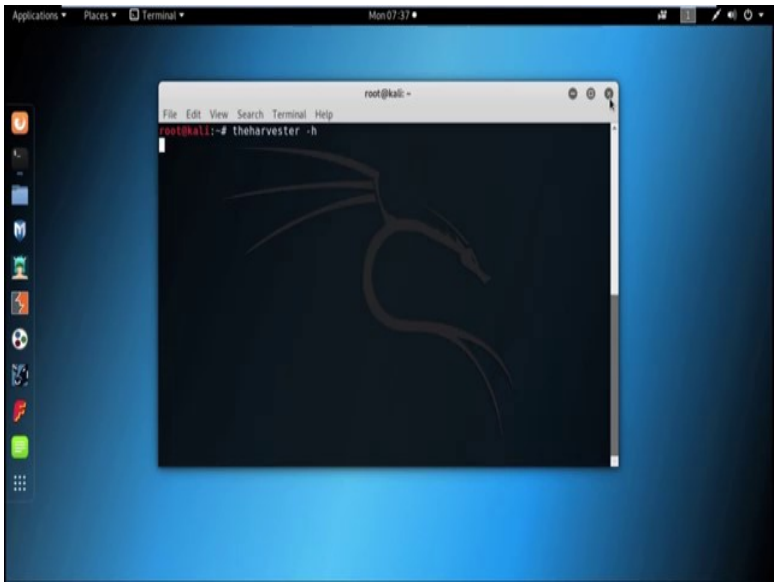
(Refer Slide Time: 16:31)



Now, check the second one. Wow it is another camera view. So, this CCTV camera is also not secured. So, like this we can find out the CCTV camera which is facing to the internet and further we can perform different attack which we will discuss in later tutorial.

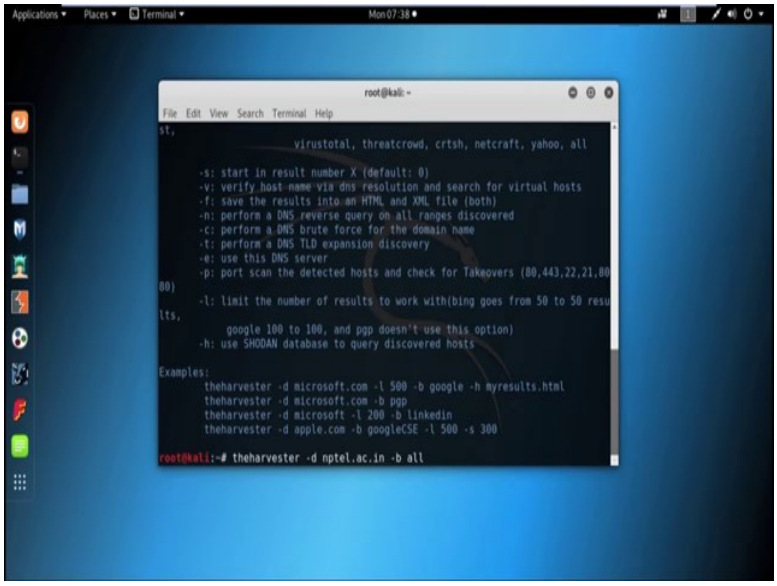
Now email harvesting using the harvester tool available in Kali Linux is an email account, username and hostname are sub domain gathering tool. As an example if you want to find email addresses and hostname for a target domain using Google we can use the tool, the harvester.

(Refer Slide Time: 18:31)

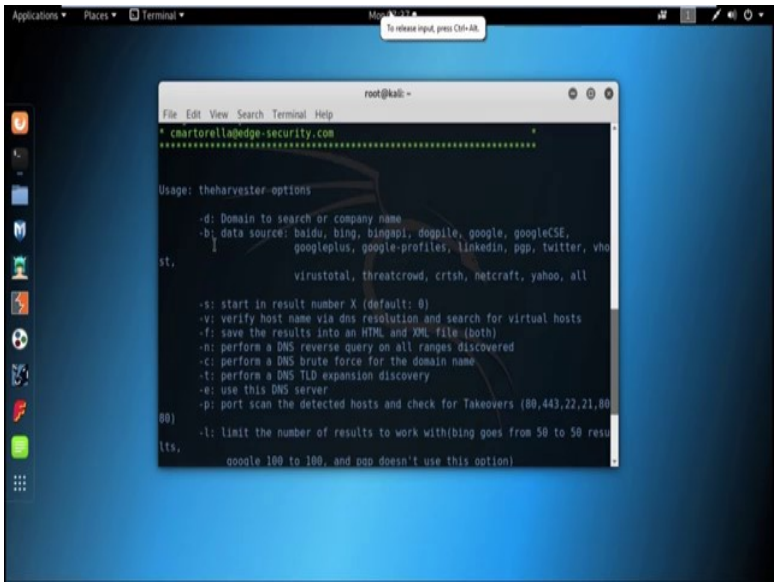


Email harvesting, the harvester tool available in Kali Linux is an email account username and hostname or sub domain gathering tool. As an example if you want to find email address and hostname for a target domain using Google, then we can use the tool the harvester. Now from terminal we can use the harvester tool. Now for help, we can use $theharvester\ -h$.

(Refer Slide Time: 19:24)

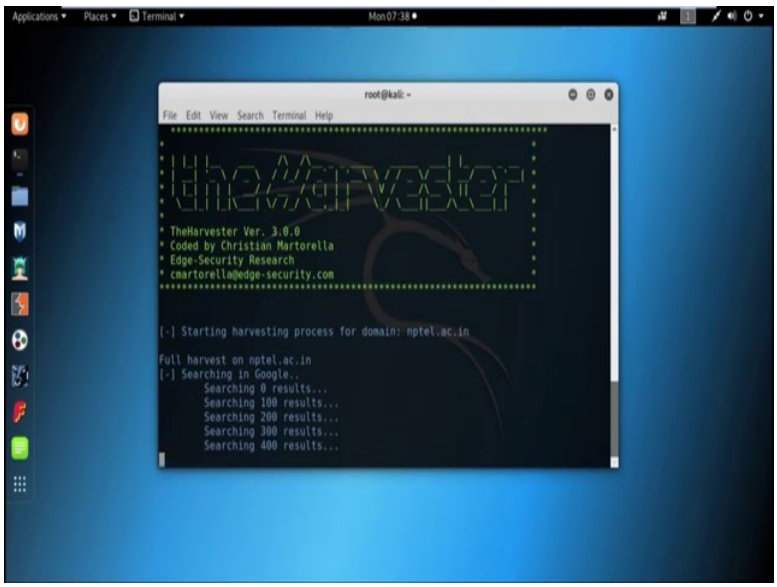


(Refer Slide Time: 19:29)



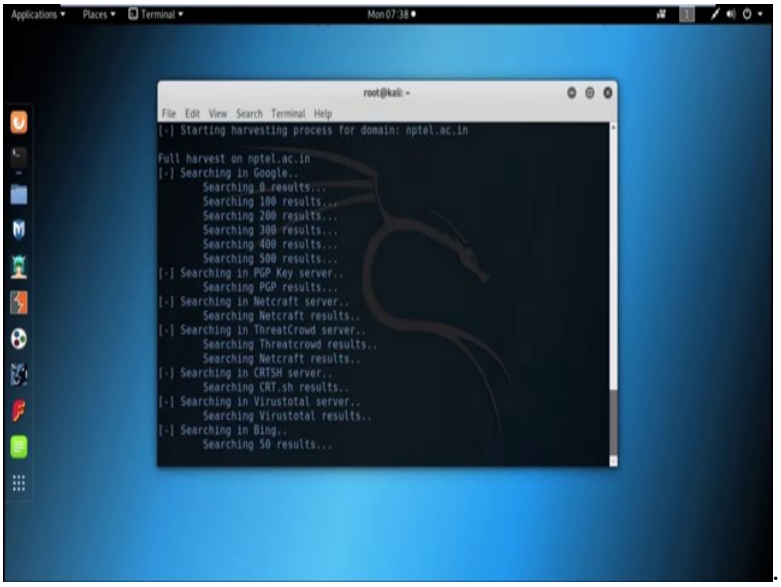
Now see to specify the domain we need to use $-d$ option and for data source like Google, linkedin pgp, twitter we need to use $-b$ option. Now, suppose I am searching all the mail id or domain name or hostname for $nptel.ac.in$. So, first we need to use the tool the harvester, then we need to specify the domain name using the parameter $-d$, say domain name is $nptel.ac.in$. Now we need to specify the data source. So, by using the $-b$ parameter we can specify the data source and by including the option, all we can include all the data source option.

(Refer Slide Time: 20:45)



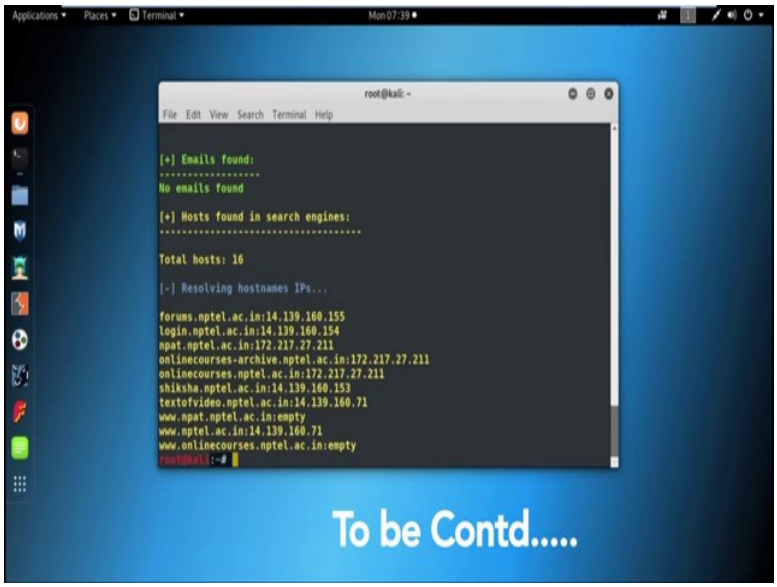
Now see the tool the harvester search for $nptel.ac.in$, it searching in Google, in pgp.

(Refer Slide Time: 20:56)



In Netcraft, Threat crowd CRISH, Virus Total, Bing and so on.

(Refer Slide Time: 21:10)



And finally we got the result. No email found and host found in search engine that is total 16 host are found with their IP address and all are listed here like $forums.nptel.ac.in$ with the IP address 14.139.160.155, then $login.nptel.ac.in$ with the IP address 14.139.160.154 and so on.