Information Security - IV
Prof. Vasan
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Module – 20
Lecture – 20
ServerSide Attacks (Contd) Tools in Kali Linux

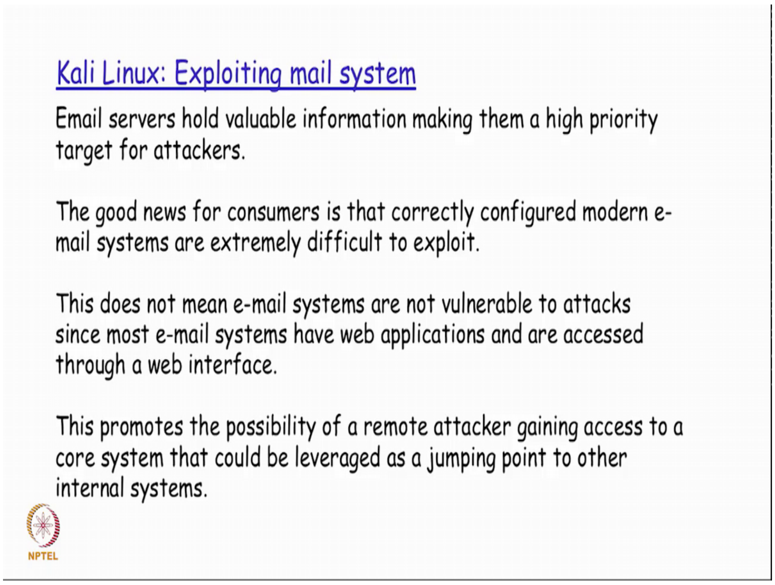
So, in this session we are going to continue looking at some more tools available in kali Linux for doing the server-side attacks. So, we have been seeing a few of the tools till now, which could potentially be used for different types of attacks on the servers, targets that has been identified as part of reconnaissance.

So, just a general note like any other tool or any other application, we would like to stress here that one needs to basically get complete hands on feeling of each other tools that we are really looking at ah, at a very, very brief level as part of the session because unless and until we really try to have those tools installed and played around with ah, it will be a little bit difficult for us to really appreciate the kind of power or the depth at each of the tools actually provides us with different kinds of features. So, as I say practise makes a man perfect.

We need to make sure that the tools that are being talked about are used as a just in as a sample reference and then along with the tools that we are looking at, all other tools related tools that we can also come out by doing our own study is all tried out and then attempted to understand basically what kind of feature that it provide, in terms of meeting our objectives of doing a very success full penetration testing.

So, we would like to request all the viewers to ensure, that those tools that we are getting discuss the are all tried out in a hands-on manner by each of you. So, that you can really get a bigger comforter feeling of how those tools work what kind of features are it is providing and how it could be used for doing a penetration testing successfully on a identified target systems

(Refer Slide Time: 02:00)



Kali Linux: Exploiting mail system

Email servers hold valuable information making them a high priority target for attackers.

The good news for consumers is that correctly configured modern e-mail systems are extremely difficult to exploit.

This does not mean e-mail systems are not vulnerable to attacks since most e-mail systems have web applications and are accessed through a web interface.

This promotes the possibility of a remote attacker gaining access to a core system that could be leveraged as a jumping point to other internal systems.

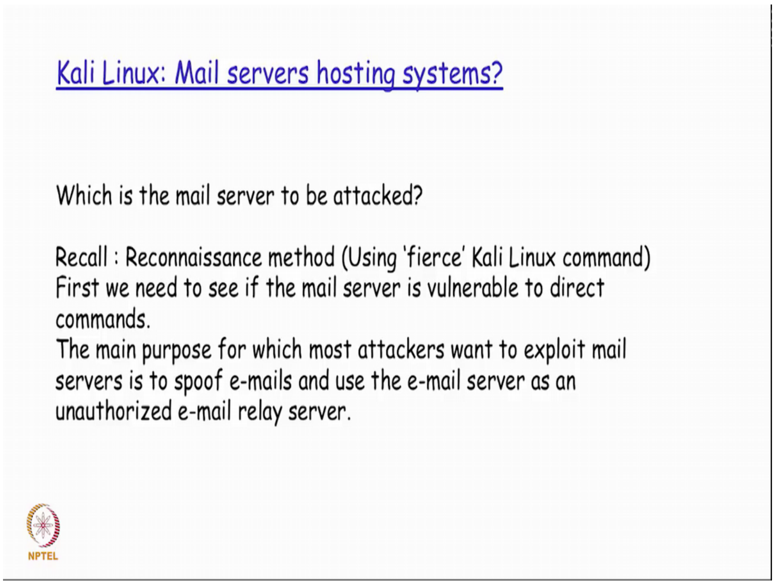
So, one of the things that could potentially be made use of as a mail system for exploitation, as we know email servers basically has details about what are the different mail accounts are there and how the email server is actually configure, using this information the person doing the penetration testing could potentially tried to make this is an entry point if at all it is considered as a very high priority at target.

Although the protocol the SMTP protocol that is predominantly used for the mail servers all through the internet. The early version of it actually had lot of loop holes; the good news is that most of the later version has actually got most of these vulnerabilities address very smartly. Email systems in most of the times over we will see that they are not sort of dedicated just for email alone, but you also would potentially have a different type of web applications that are actually used, installed and used on the same system which would be actually access over a web interface from the internet.

So, because of this particular fact it basically opens up a bigger possibility of having more vulnerabilities on that same system, which could potentially be made use of by as an attack by the attacker as an entry point for him to basically jump to other exam to other internal systems of that same network in which the system is present.

How was how does one actually try to attack a mail server?

(Refer Slide Time: 03:40)



Kali Linux: Mail servers hosting systems?

Which is the mail server to be attacked?

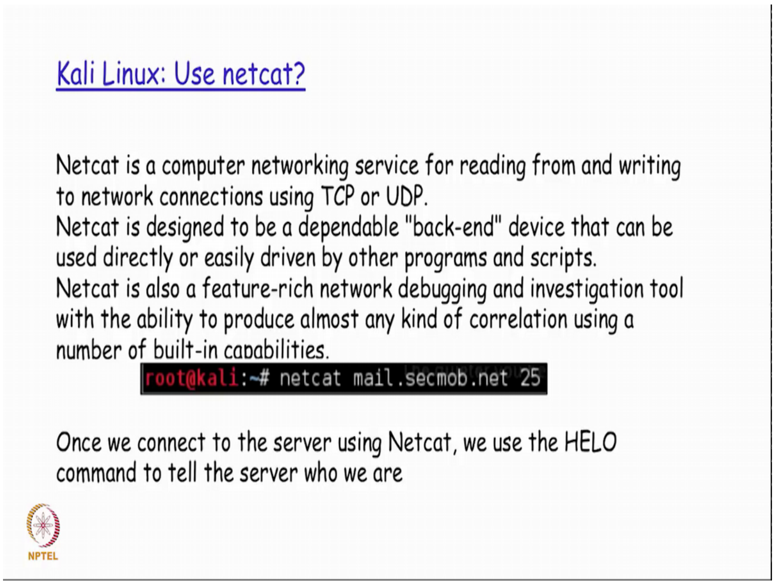
Recall : Reconnaissance method (Using 'fierce' Kali Linux command)
First we need to see if the mail server is vulnerable to direct commands.
The main purpose for which most attackers want to exploit mail servers is to spoof e-mails and use the e-mail server as an unauthorized e-mail relay server.

So, if you recall in the reconnaissance method we basically had the look that different tools; with which will with which we will be able to find out more details about what are all the different servers it is actually configure the DNS system, right? So, the fierce was basically the kali Linux tool that we had actually look that, and one of their sub domains which will typically be there in any domain registration will be the corresponding mail server registration, right?

So, with m x record of the DNS corresponding to the mail server, if you have for example, Google dot com we all know that there is something called as mail dot Google dot com, right? Likewise using the fierce tool that is available in kali Linux we saw how the different sub domains within a particular registered domain could actually be found out, and mail server will be one of those domains typically, right?

So, one of the main reasons why attack I would want to basically exploit a mail server is to sort of spoof emails as of the mails are got generated from some other person, right?

(Refer Slide Time: 04:41)



Kali Linux: Use netcat?

Netcat is a computer networking service for reading from and writing to network connections using TCP or UDP.
Netcat is designed to be a dependable "back-end" device that can be used directly or easily driven by other programs and scripts.
Netcat is also a feature-rich network debugging and investigation tool with the ability to produce almost any kind of correlation using a number of built-in capabilities.

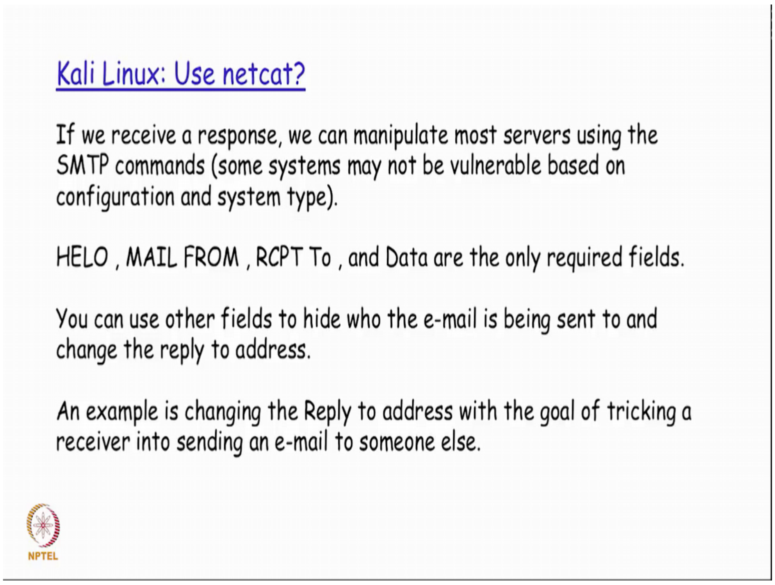
```
root@kali:~# netcat mail.secmob.net 25
```

Once we connect to the server using Netcat, we use the HELO command to tell the server who we are

So, one of the things that we could actually make use of as a tool called the netcat so, netcat is basically computer networking service, that basically helps one in trying to read and write a TCP or UDP connection, right? So, we already know what is a TCP or UDP connection from our previous I s 3. So, netcat could actually be used to design a very dependable application on top of a, with which you would be able to do a read and write on either a TCP or UDP based connection, right? So, if you for example, say netcat mail dot secmob dot net and followed by the port number. Port number 25 as most of us would know is a well-known port that is typically used by my SMTP mail servers across. So, that is that is that is actually the default well known port port number that is actually used for the mail server.

So, once we connect to the server using netcat we could actually make use the hello command to tell the server we are who we are right?

(Refer Slide Time: 05:44)



Kali Linux: Use netcat?

If we receive a response, we can manipulate most servers using the SMTP commands (some systems may not be vulnerable based on configuration and system type).

HELO , MAIL FROM , RCPT To , and Data are the only required fields.

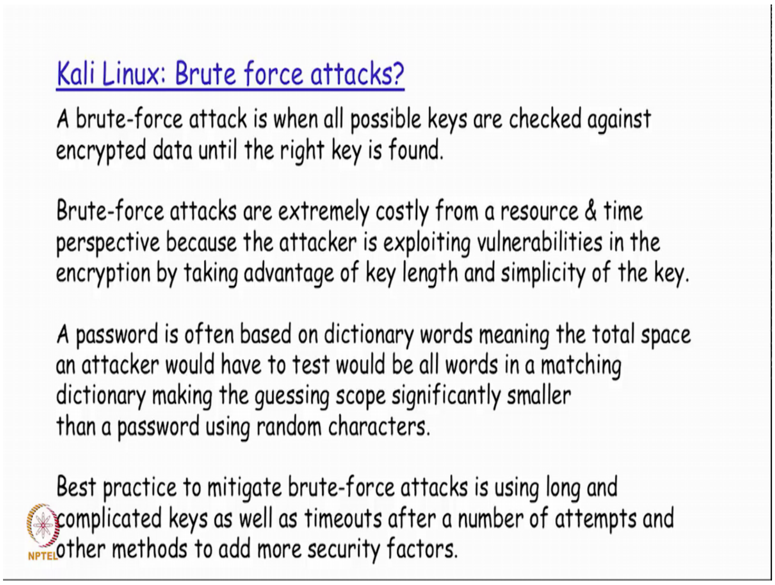
You can use other fields to hide who the e-mail is being sent to and change the reply to address.

An example is changing the Reply to address with the goal of tricking a receiver into sending an e-mail to someone else.

So, after that I could basically go ahead and try to use a mail from receive to and all these things, which is basically what a typically an email client would actually do after getting all these details from the user, right? So, when we actually type a mail compose a mail saying the 2 field is whatever is the 2 address to which you want to send the mail, that particular email address is actually mark does an argument to the receipt to SMTP mail server command.

So, with all these SMTP commands that I could get free found out on the SMTP RFC. I could actually generate email automatically using this kind of an application like netcat and I could basically send an email as if it originated from somebody. And also, could use potentially the reply to field differently. So, that when that particular email is getting replied without the person possibly realizing that it is actually getting generated the reply is getting generated to another email address, the mail will the reply mail will actually come to another email address that is actually getting marked as the reply to address of this new composed mail .

(Refer Slide Time: 06:53)



Kali Linux: Brute force attacks?

A brute-force attack is when all possible keys are checked against encrypted data until the right key is found.

Brute-force attacks are extremely costly from a resource & time perspective because the attacker is exploiting vulnerabilities in the encryption by taking advantage of key length and simplicity of the key.

A password is often based on dictionary words meaning the total space an attacker would have to test would be all words in a matching dictionary making the guessing scope significantly smaller than a password using random characters.

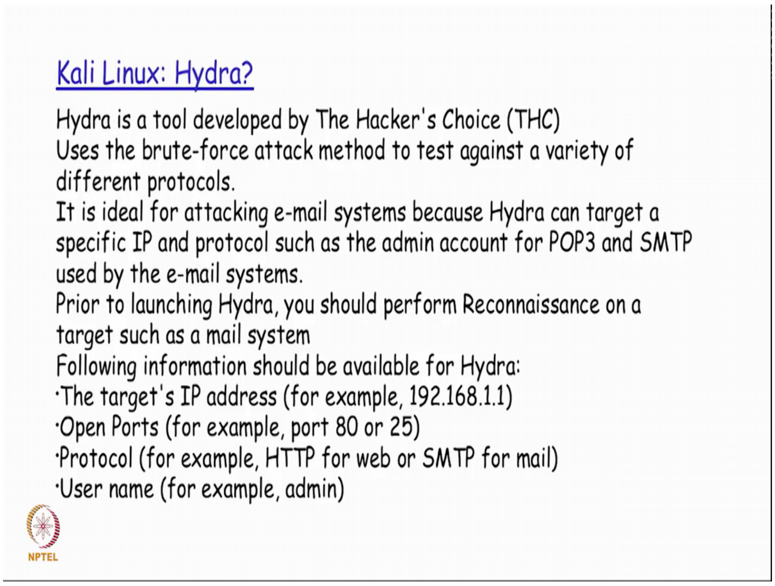
Best practice to mitigate brute-force attacks is using long and complicated keys as well as timeouts after a number of attempts and other methods to add more security factors.

Coming down into the last part of the serverside attacks now going to start looking at what is called as a brute force attack. The brute force attack is basically when I try to as an attacker try to find out in brute force manner may be the user I d is on the passwords are the keys for whatever it is, that would help me to successfully get myself authenticated into that particular targeted system, right?

Going by the nature as we as we can very easily understand, all kinds of brute force testing are very, very computational intensive; meaning that it will actually take a lot of time and lot of resources for that occurred to basically have the brute force testing completed successfully to it is full completion level, right? so for this particular reason you will always find that the administrators of your servers or your network portal whatever it is basically, advise you to actually have a very long password, because the longer the password longer the key if a potential attackers actually trying to employee the brute force mechanism it is going to take him that much long period of time for him to successfully get what is the password or the username or the key that he is actually trying to get.

The shorter the password length the quicker will it will you be able to get the key of the password and the longest length we can vary naturally imagine, how difficult it will be for him in terms of the amount of time that he has to wait before he is even possible possibly successful in getting the key or the password, right? So, in addition the more the bigger the key it is going to take more time for the for the attacker to basically get access to the key by which time, we can hope that the alerts basically start getting triggered off for the administrator to realise that some kind of a brute force attack is possibly getting initiated and is possibly in progress right now on that system, after which administrator can take some quick termination actions, right?

(Refer Slide Time: 09:06)



Kali Linux: Hydra?

Hydra is a tool developed by The Hacker's Choice (THC)
Uses the brute-force attack method to test against a variety of different protocols.
It is ideal for attacking e-mail systems because Hydra can target a specific IP and protocol such as the admin account for POP3 and SMTP used by the e-mail systems.
Prior to launching Hydra, you should perform Reconnaissance on a target such as a mail system
Following information should be available for Hydra:

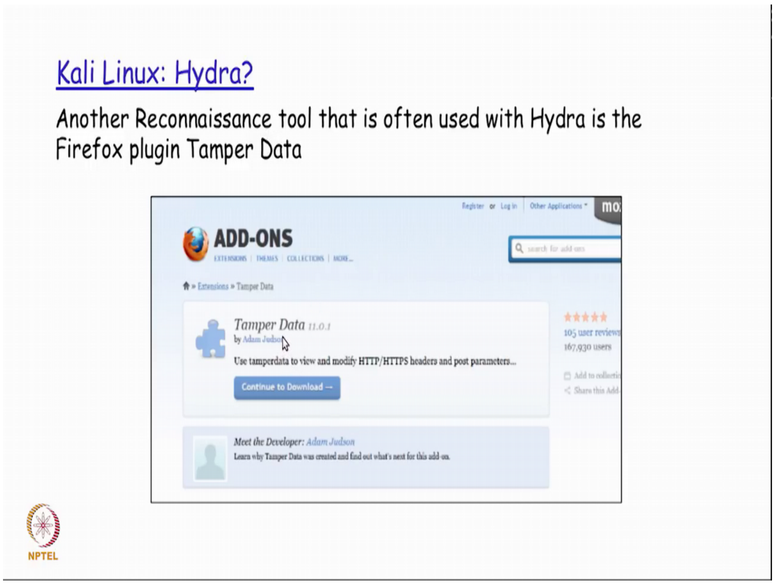
- The target's IP address (for example, 192.168.1.1)
- Open Ports (for example, port 80 or 25)
- Protocol (for example, HTTP for web or SMTP for mail)
- User name (for example, admin)

So, always it is there is a best practice from a defence mechanism to have a very big password and not really have it as part of something like a dictionary password string something which is better be available from a dictionary or the user name itself on so and so for, right? So, hydra is basically tool that is actually available for doing a different types of a brute force attacks. So, it is a typically used for attacking an image system because hydra can take an ip address to the target.

And it could also try to break in the administrator account for pop 3 or SMTP protocol used by the email system so, right? So, what kind of information should be available for hydra we need the targets ip address? We need what are the open port. So, whether it is a port number 80 or 443 or 25 or whatever is a open port. And what is the protocol that is actually going to be used? So, whether we are going to just use HTTP or whether we going to use a SMTP and so on. And also, what is the typical user name that has got to be use.

So, for example, it could be admin or administrator or whatever it is. So, this kind of details are required for this particular tool, which could potentially be part of my output from my reconnaissance step right so on that particular mail system. So, for the hydra to work us actually need a Firefox plugin tool call tamper data.

(Refer Slide Time: 10:35)



Kali Linux: Hydra?

Another Reconnaissance tool that is often used with Hydra is the Firefox plugin Tamper Data

Register or Log in | Other Applications
ADD-ONS
EXTENSIONS | THEMES | COLLECTIONS | MORE...
search for add-ons
Extensions » Tamper Data

Tamper Data 11.0.1
by Adam Judson

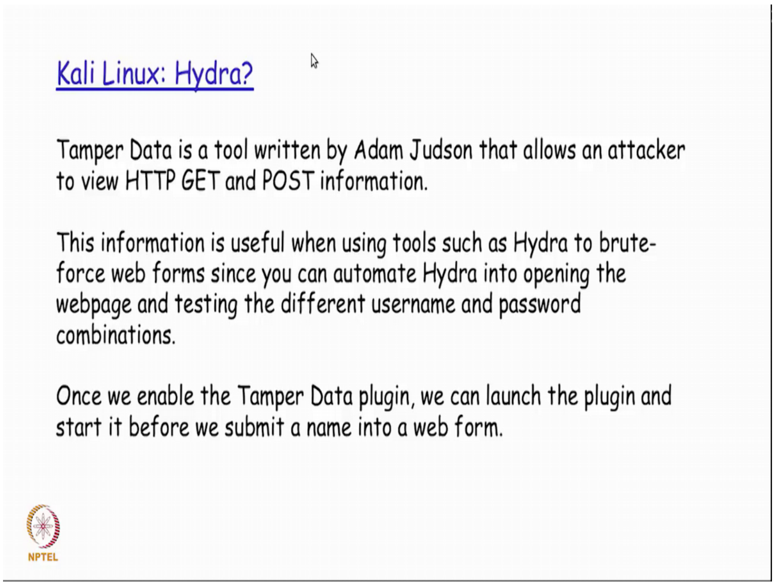
Use tamperdata to view and modify HTTP/HTTPS headers and post parameters...

105 user reviews
167,930 users

Meet the Developer: Adam Judson
Learn why Tamper Data was created and find out what's next for this add-on.

So, this is something which is actually downloadable and installable within Firefox as an Firefox add on. And it is also a very popular tool that we could actually easily install, right?

(Refer Slide Time: 10:47)



Kali Linux: Hydra?

Tamper Data is a tool written by Adam Judson that allows an attacker to view HTTP GET and POST information.

This information is useful when using tools such as Hydra to brute-force web forms since you can automate Hydra into opening the webpage and testing the different username and password combinations.

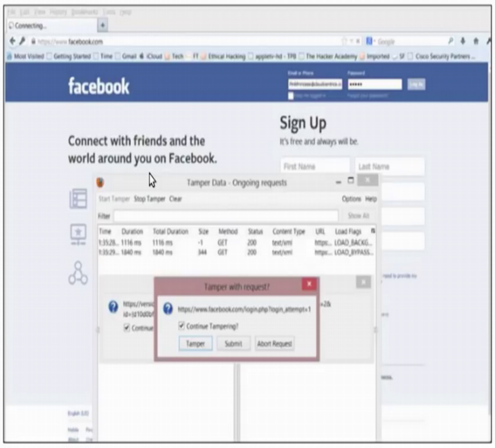
Once we enable the Tamper Data plugin, we can launch the plugin and start it before we submit a name into a web form.

So, tamper data is basically a tool return by Adam Judson. that basically helps an attacker to sort of get details from a GET and POST method of HTTP protocol, right? So, as some of us know the GET in the POST method of a HTTP protocol is typically used for getting the day form getting the page details or taking input details from the form, and then posting it on to the remote server.

So, the details that is actually available as part of this tamper data plugin, will be used by tool like hydra a for it to essentially reduce the kind of complexity on the time of effort type of effort for that is typically required for doing a very long fetched brute force attack.

(Refer Slide Time: 11:35)

Kali Linux: Tamper Data plugin?



Tamper Data - Ongoing requests

Time	Duration	Total Duration	Size	Method	Status	Content Type	URL	Load Flags
1:35:28...	1116 ms	1116 ms	-1	GET	200	text/xml	https:...	LOAD_BACKG...
1:35:29...	1840 ms	1840 ms	344	GET	200	text/xml	https:...	LOAD_BYPASS...

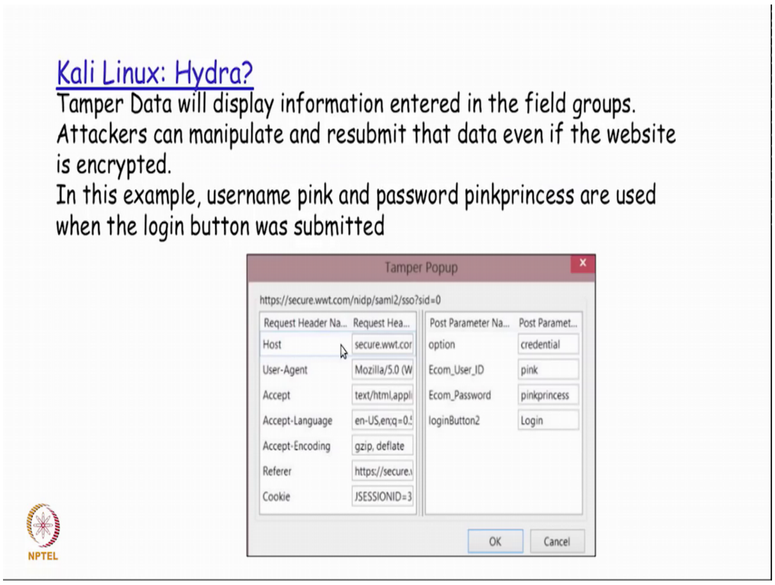
Tamper with request?

https://www.facebook.com/login.php?login_attempt=1

☑ Continue Tampering?

The inputs that is actually provided by the tamper data, will be used for generating the different username and password combinations into the hydra tool. So, this is basically how we actually make use of the tamper data. So, before we actually I have the user name and password typed in; we enable the tamper data plugin and then sort of accept and say for the tamper to be enabled. So, once it is done.

(Refer Slide Time: 12:00)



Kali Linux: Hydra?

Tamper Data will display information entered in the field groups. Attackers can manipulate and resubmit that data even if the website is encrypted.

In this example, username pink and password pinkprincess are used when the login button was submitted

Tamper Popup

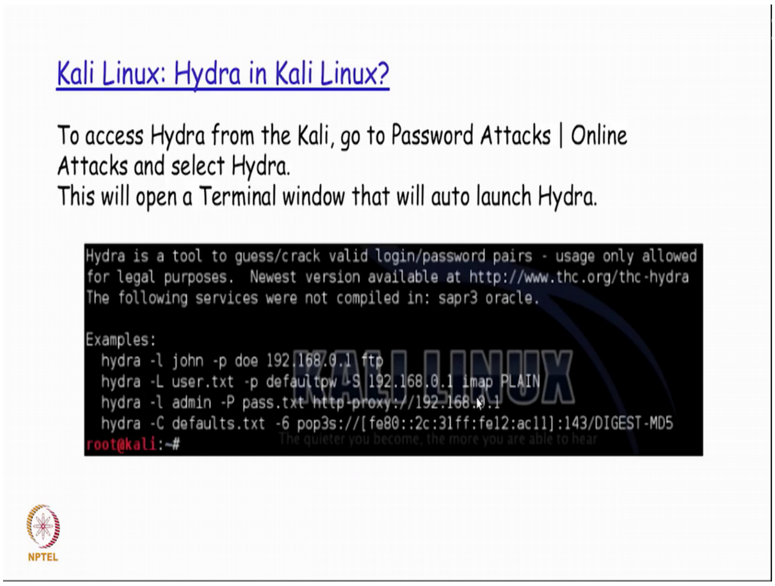
https://secure.wwt.com/nidp/saml2/sso?sid=0

Request Header Na...	Request Hea...
Host	secure.wwt.cor
User-Agent	Mozilla/5.0 (W
Accept	text/html,appli
Accept-Language	en-US,en;q=0.!
Accept-Encoding	gzip, deflate
Referer	https://secure.\
Cookie	JSESSIONID=3

Post Parameter Na...	Post Paramet...
option	credential
Ecom_User_ID	pink
Ecom_Password	pinkprincess
loginButton2	Login

We actually have a popup on displayed on the screen whenever there is a username and password that is entered. And that is a potential username password that will be actually getting printed here; that has been recognised as part of this plugin of tamper data, right?

(Refer Slide Time: 12:21)



Kali Linux: Hydra in Kali Linux?

To access Hydra from the Kali, go to Password Attacks | Online Attacks and select Hydra.

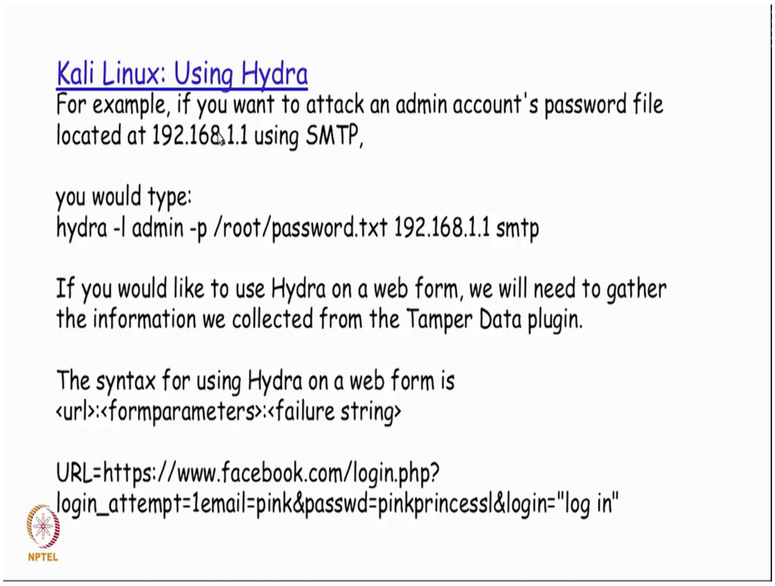
This will open a Terminal window that will auto launch Hydra.

```
Hydra is a tool to guess/crack valid login/password pairs - usage only allowed
for legal purposes.  Newest version available at http://www.thc.org/thc-hydra
The following services were not compiled in: sapr3 oracle.

Examples:
  hydra -l john -p doe 192.168.0.1 ftp
  hydra -L user.txt -p defaultpw -S 192.168.0.1 imap PLAIN
  hydra -l admin -P pass.txt http-proxy://192.168.0.1
  hydra -C defaults.txt -6 pop3s://[fe80::2c:31ff:fe12:ac11]:143/DIGEST-MD5
root@kali:~#
```

So, once this is done it basically becomes very easy for tool like hydra tool actually work in. So now, where is hydra tool available is that it could actually it could actually go under password attacks menu in kali Linux applications menu option. And then go inside the online attacks and select hydra which is listed as one of the tools that is there as part of the sub menu. So, once you select this particular sub menu option it open the terminal window and we have details about the possible ways by which, the hydra tool could actually be used as part of the welcome screen.

(Refer Slide Time: 12:56)



Kali Linux: Using Hydra

For example, if you want to attack an admin account's password file located at 192.168.1.1 using SMTP,

you would type:

```
hydra -l admin -p /root/password.txt 192.168.1.1 smtp
```

If you would like to use Hydra on a web form, we will need to gather the information we collected from the Tamper Data plugin.

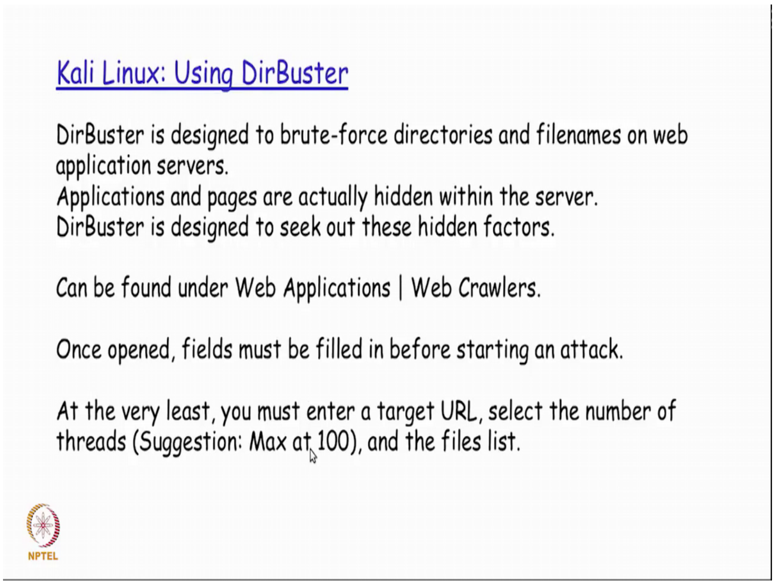
The syntax for using Hydra on a web form is
<url>:<formparameters>:<failure string>

URL=https://www.facebook.com/login.php?
login_attempt=1email=pink&passwd=pinkprincessl&login="log in"

So, I could actually either use it in one form if I basically decide if I basically want have SMTP as a protocol, by which I just say hydra and I give the administrator password name. And then I give the possible password text files, right? So, this name I basically get it from a tamper data plugin, and then whatever are the possible password that is there a part of my dictionary I actually have it put in a particular file and then give this is an argument to the minus p option when I invoke hydra in the command line, right? And then I specify the ip address and then I also specify what protocol here. So, if I am basically trying to have SMTP as a protocol ah.

So, I could actually specify SMTP here, and then the this particular tool will actually start the brute force testing method of trying to identify; every password it is actually mentioned in the given file for that particular user name admin on that SMTP server of 1.1 192.168.1.1. Similarly, I could also use it as a web form, in this manner by which I could basically specify the URL in this particular string and then give that for a starting hydra.

(Refer Slide Time: 14:11)



Kali Linux: Using DirBuster

DirBuster is designed to brute-force directories and filenames on web application servers.
Applications and pages are actually hidden within the server.
DirBuster is designed to seek out these hidden factors.

Can be found under Web Applications | Web Crawlers.

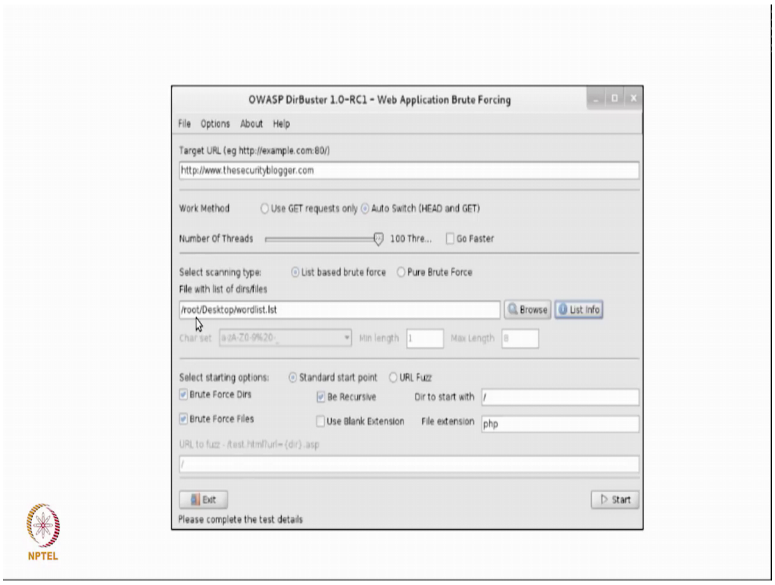
Once opened, fields must be filled in before starting an attack.

At the very least, you must enter a target URL, select the number of threads (Suggestion: Max at 100), and the files list.

Now another brute force tool that is actually available is what is called as a DirBuster. So, DirBuster is basically a tool that will help that the attacker to find out the entire directory structure, right? And other possible list of file names in the subdirectory tree right? In typical web application server, we would find that from the URL field you could find that there is a huge sometimes are the URL is actually very large, and the large part of the URL will basically also give as an idea on what is the entire directory tree that is actually available as part of this particular web server, right?

So, applications and pages could potentially be hidden within the server. So, this particular tool called dirbuster is basically designed designed to sort of unhide all those hidden applications and web pages that an attacker would possibly need as part of his testing effort, right? So, this particular tool will be available under web applications menu and submenu of web crawlers. So, DirBuster tool will actually listed as part of the web crawler submenu. So, once this particular tool is open that are different fields that it is actually got to be entered in the menu option. So, first and foremost is, what is the URL that needs to be targeted.

(Refer Slide Time: 15:33)



OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

Target URL (eg http://example.com:80/)
http://www.thesecurityblogger.com

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 100 Thre... □ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files
/root/Desktop/wordlist.lst

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

Select starting options: ● Standard start point ○ URL Fuzz

☑ Brute Force Dirs ☑ Be Recursive Dir to start with /

☑ Brute Force Files □ Use Blank Extension File extension php

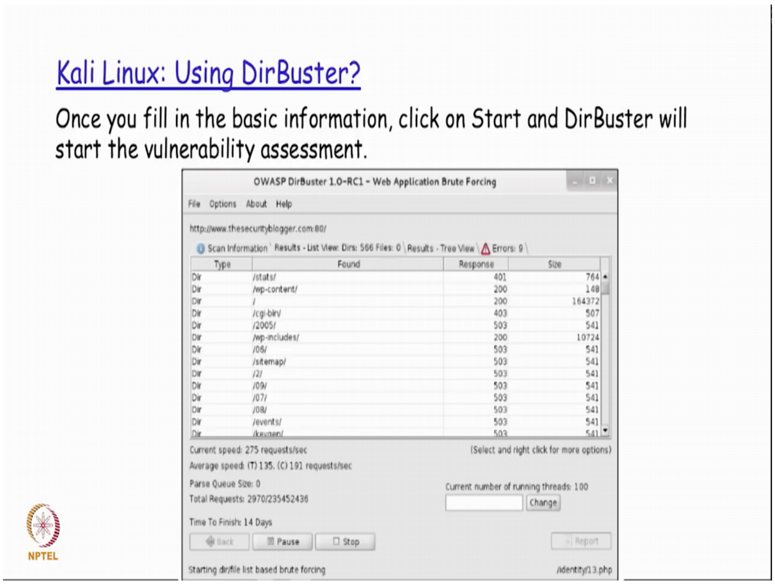
URL to fuzz - /test.html?url={dir}.asp
/

Please complete the test details

And you could also specify a file which will typically contain the list of file or the directory name that it has to be searched with inside this particular web server, right?

So, once you give this particular URL and we also specify this name. you could basically a start it with the pay the scanning effort to find out which among the strings in this particular given input file is actually available as part of the entire directory tree of this web server, right? There also have a number of threads that is there. So, you could possibly have maximum of 100 threads that is basically what a recommendation would be or select even lesson number of threads depending on the hardware configuration of a particular system, and how much of a memory space you would really have, right? So, once you give this input parameters and then says start.

(Refer Slide Time: 16:26)



Kali Linux: Using DirBuster?

Once you fill in the basic information, click on Start and DirBuster will start the vulnerability assessment.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

http://www.thesecurityblogger.com:80/

Type	Found	Response	Size
Dir	/stats/	401	764
Dir	/wp-content/	200	148
Dir	/	200	164372
Dir	/cgi-bin/	403	507
Dir	/2005/	503	541
Dir	/wp-includes/	200	10724
Dir	/06/	503	541
Dir	/sitemap/	503	541
Dir	/2/	503	541
Dir	/09/	503	541
Dir	/07/	503	541
Dir	/08/	503	541
Dir	/events/	503	541
Dir	/keygen/	503	541

Current speed: 275 requests/sec

(Select and right click for more options)

Average speed: (T) 135, (C) 191 requests/sec

Parse Queue Size: 0

Total Requests: 2970/235452436

Current number of running threads: 100

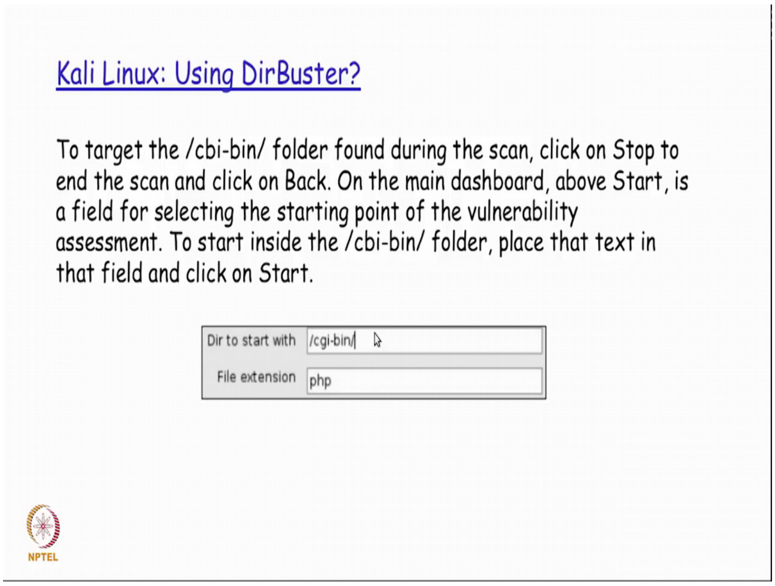
Time To Finish: 14 Days

Starting dir/file list based brute forcing

/identity/13.php

The tool basically start running and then it basically gives you the different kinds of subdirectories that it is actually found in this particular website. So, in this particular website on port number 80 it basically tells that it is actually having so many different subdirectories at it is found. And the moment you want to have specific details on a single subdirectory that it is already out. You could actually potentially press the stop button and then press the field of the directory what directory to start with as this particular directory that you are requiring.

(Refer Slide Time: 16:57)



Kali Linux: Using DirBuster?

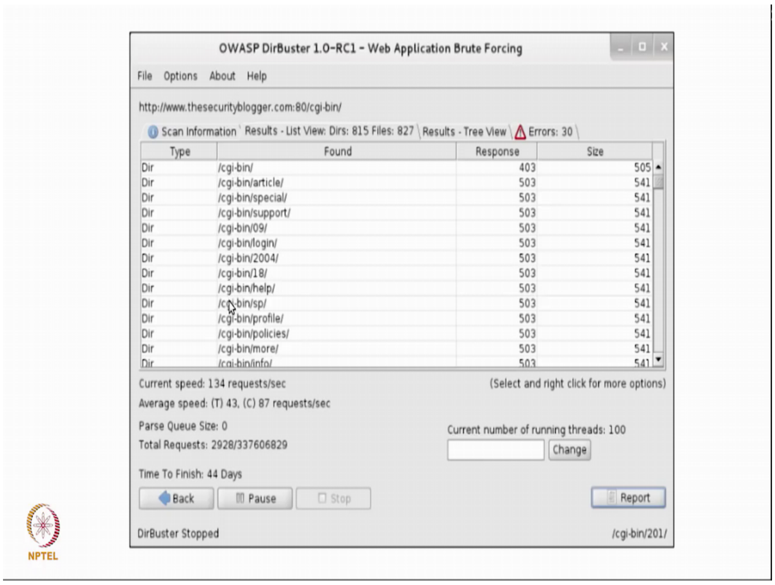
To target the /cbi-bin/ folder found during the scan, click on Stop to end the scan and click on Back. On the main dashboard, above Start, is a field for selecting the starting point of the vulnerability assessment. To start inside the /cbi-bin/ folder, place that text in that field and click on Start.

Dir to start with /cgi-bin/

File extension php

So, if you have already the tool is already reported that cgi-bin is a directory in which is actually available as a subdirectory in that particular web server. So, you could actually specify cgi-bin as the directory to start with in this particular menu option in the main dashboard. And also if you have a very specific requirement of only trying to find out some specific files with the particular extension, you could also populated it in the next textbox at is there. So, you want to for example, find only php files on img files or whatever it is; that I could basically place that text in this particular field then say start for it to basically have that particular scan started specifically in the selected directory, right?

(Refer Slide Time: 17:44)


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
Scan Information
Results - List View: Dirs: 815 Files: 827
Results - Tree View
Errors: 30
Change
Back
Pause
Stop
Report
NPTEL

http://www.thesecurityblogger.com:80/cgi-bin/

Type	Found	Response	Size
Dir	/cgi-bin/	403	505
Dir	/cgi-bin/article/	503	541
Dir	/cgi-bin/special/	503	541
Dir	/cgi-bin/support/	503	541
Dir	/cgi-bin/09/	503	541
Dir	/cgi-bin/login/	503	541
Dir	/cgi-bin/2004/	503	541
Dir	/cgi-bin/18/	503	541
Dir	/cgi-bin/help/	503	541
Dir	/cgi-bin/sp/	503	541
Dir	/cgi-bin/profile/	503	541
Dir	/cgi-bin/policies/	503	541
Dir	/cgi-bin/more/	503	541
Dir	/cgi-bin/info/	503	541

Current speed: 134 requests/sec (Select and right click for more options)

Average speed: (T) 43, (C) 87 requests/sec

Parse Queue Size: 0

Total Requests: 2928/337606829

Current number of running threads: 100

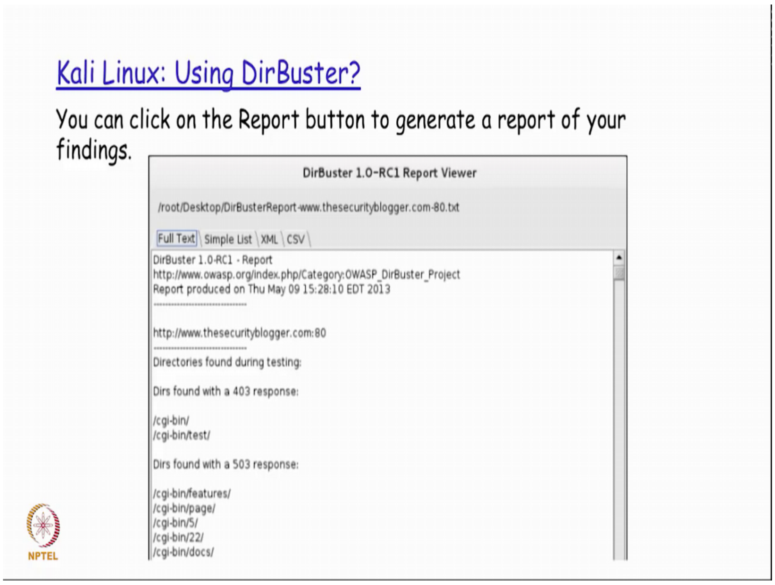
Time To Finish: 44 Days

DirBuster Stopped

/cgi-bin/201/

So, if you are selected cgi-bin now the output will only contain things that is actually been found out as part of sub directories or files under the cgi-bin directory alone. So, that is basically what you will find in the output that is presented as part of the tool output.

(Refer Slide Time: 18:03)



Kali Linux: Using DirBuster?

You can click on the Report button to generate a report of your findings.

/root/Desktop/DirBusterReport-www.thesecurityblogger.com-80.txt

```
DirBuster 1.0-RC1 - Report
http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
Report produced on Thu May 09 15:28:10 EDT 2013
--------------------------------

http://www.thesecurityblogger.com:80
--------------------------------
Directories found during testing:

Dirs found with a 403 response:

/cgi-bin/
/cgi-bin/test/

Dirs found with a 503 response:

/cgi-bin/features/
/cgi-bin/page/
/cgi-bin/5/
/cgi-bin/22/
/cgi-bin/docs/
```

So, the tool also basically gives your report on so if you click on the report button that is there in the tool like the start button and everything. It basically generate the report the findings that has been done till now. So, it tells you how many days have been found how many files have been found, and what day has been found, that what different HTTP responses like a 503 response or a 4 naught 4 response so on.

So, if you for example, know that some it have got a 404 response, you would know that that particular folder name is actually not available as part of this particular directory tree of this URL, right? So, that way this report basically gives you a mechanism to get more details about this particular portal.

Thank you.