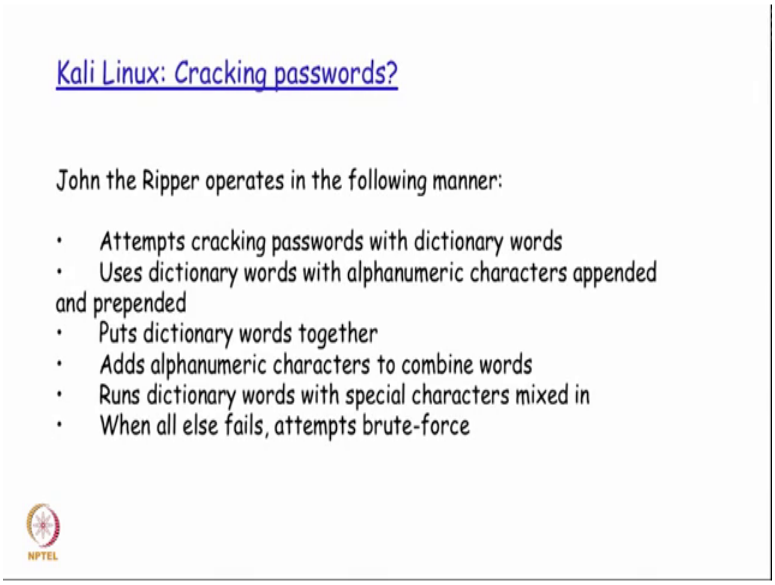
Information security - IV
Prof. Vasan
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Module - 22
Lecture – 22
Server Side Attacks (Contd)
Tools in Kali Linux

So, this session we are going to continue seeing some more tools on the server side a penetration testing attacks that could potentially be we made use of. So, we are getting into starting to look at what kind of tools, are actually available for cracking the password.

(Refer Slide Time: 00:35)



Kali Linux: Cracking passwords?

John the Ripper operates in the following manner:

- Attempts cracking passwords with dictionary words
- Uses dictionary words with alphanumeric characters appended and prepended
- Puts dictionary words together
- Adds alphanumeric characters to combine words
- Runs dictionary words with special characters mixed in
- When all else fails, attempts brute-force

So, as part of this particular course we are going to see quite a few tools and techniques that are typically used for trying to do a sort of a cracking or brute force attacking a particulars targeted server for getting to know what passwords are used. And one of the most popular tools that is commonly used for cracking the passwords is what is called as John the Ripper right. So, John the Ripper is a very famous tool and this is a tool that is actually available also as part of Kali Linux.

So, it tries to sort of operate in a following manner and the kind of steps that it actually takes to find out what is the password for the different users on a particular system is very very comprehensive right. So, the more the amount of time that we actually give to the tool, you will find that it is actually that much more successful in determining the the password in a brute force method. So, how exactly does this operate?

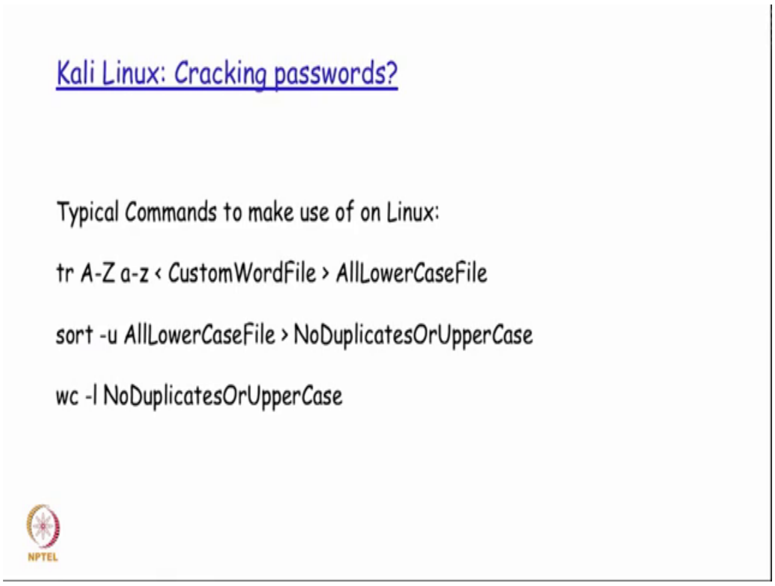
So, basically tries to crack the password with standard dictionary words. So, if you actually tried to have a password, which is exactly as given in any of the standard dictionaries right it will first try to find that out and there by it will find it very easy to crack the password and then also displayed right now if this is not successful. So, if it has actually exploited all the passwords that is actually available as part of the dictionary, and still if it has not been successful in it. It is going to basically use the dictionary word combined with alphanumeric characters appended to wait or either prepended to yet right. So, any kind of you know alphanumeric characters.

So, a number for example, could be either appended to a dictionary word or prepended to dictionary word, and then it will try to find out if that is something which is going to be which is actually been used as the password for a particular user right. If that is also not successful then next step that it will actually try to do is it will randomly pick up two different dictionary words together, and combine them to see if it is something which is actually being used as a password right. And then on the combined words suppose if this is not successful, on the combined words it actually tries to add up alphanumeric characters either at the beginning or at the end, and even if this is not successful it is actually going to start randomly inserting a special characters mixed inside the entire string right.

So, the special characters could be a any any any any kind of a printable characters that is available in your normal keyboard, and then if all of these specific combinations fail it is then going to start doing a brute force method. So, from this list of options you could very clearly see, how comprehensively it is trying to attempt to crack the password and that is basically the reason why one it actually takes a long time to complete, and number 2 its also the reason why most of the servers and portals basically ask you to keep very secure passwords with very cryptic formats are saying that one minimum capital letter and one small letter and one punctuation character, one number and so on and so forth right.

So, we all have experienced this in different portals, where we are forced to actually have a password string which is not very easily crackable by this kind of tools. So, that is again we should understand is the reason why because of the presence of these tools, the portals basically force the users to ensure that they actually have very long and very cryptic passwords operate not to be get not not to be getting easily cracked.

(Refer Slide Time: 04:42)



Kali Linux: Cracking passwords?

Typical Commands to make use of on Linux:

```
tr A-Z a-z < CustomWordFile > AllLowerCaseFile

sort -u AllLowerCaseFile > NoDuplicatesOrUpperCase

wc -l NoDuplicatesOrUpperCase
```

So, when we actually try to crack the passwords what we actually do is we referred to dictionary files that are present and available in a lot of places in the internet right. So, the moment you actually try to download multiple dictionary files from different sources, what could potentially happen is that there could be duplicate sign it.

So, one string that is actually represent in one dictionary will also be possibly present in lets say dictionary number 10. So, you want to actually eliminate all those duplicates. So, that unnecessarily the tool does not waste the time, when it is actually searched for that particular password earlier. So, for this particular purpose we actually run a few commands on the downloaded dictionary files from the internet, whenever we download multiple dictionary files on the internet.

So, the first command that we actually run is what is called as the tr command. This tr command basically stands for it is lyrics command that is actually stands for translate. So, it basically translates all the characters capital A to capital Z into small a to small z.

So, a capital B anywhere in any of the strings will actually be getting replaced with the small letter b in that particular word.

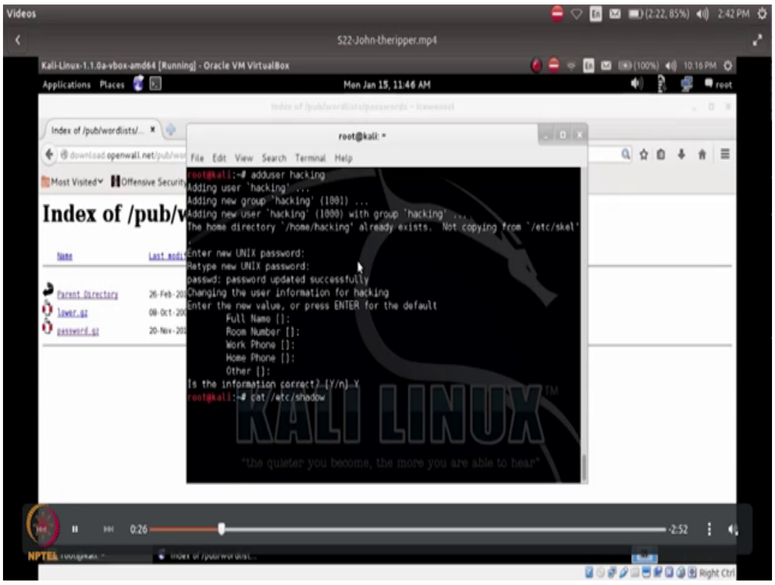
So, what we actually do here is that. So, as an input we basically pass the file that we have actually downloaded from different places concatenated all of them together into a single file. So, this particular file custom word file is an input that is passed to the command and this command is going to substitute all capital letters with small letters, and then redirect the content into another file with this name called all lowercase file. So, this is basically what this particular Linux command is actually doing.

So, the idea here is that by running this command we sort of make sure that we only one word in one single case pattern uniformly. So, if I basically have a have a let us a string called read me one string called read me all in lowercase and another string called read me all uppercase, this is basically going to convert the uppercase read me string into all letters with lower case right. Now after having done that, there is a possibility that I am going to have a duplicates. So, what we do is, with then run the command called sort. So, the sort command with the option of minus u will basically remove all redundant strings that is actually present in the given input file, because that is basically what we want to finally, used for the dictionary file as an input into the tool right.

So, you basically do a sort command on that file on that file with minus u option to remove all redundancies, and then redirect that output into another file called no duplicates or uppercase file. So, this particular name file name is no not go is now it is now not going to have any duplicate strings, and also there will be no strings with uppercase in it and it all be only with lower cases. So, then finally, for getting an idea of how many words are there you could run the wc minus l command to get the number of lines in that in that file which will tell us how many strings are present in that entire file, which the tool is actually going to make use of for doing the brute force cracking of the password.

So, with a very small video demo let us see how this tool is actually working.

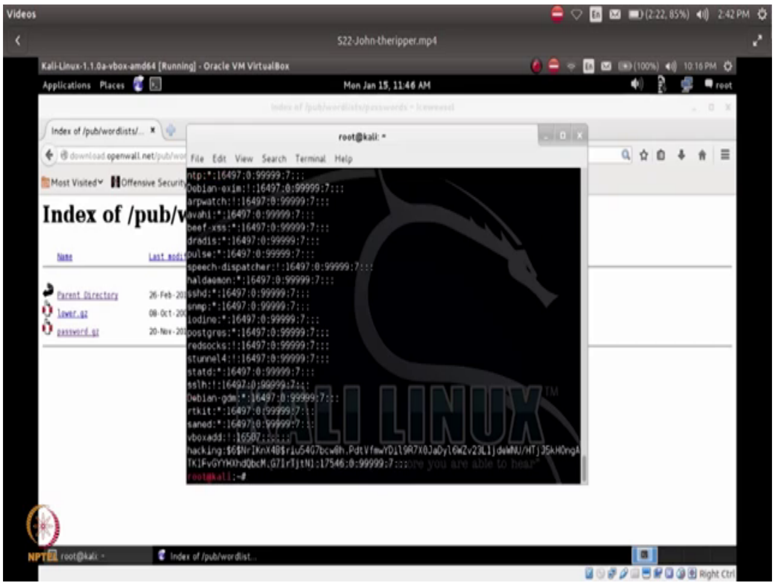
(Refer Slide Time: 08:13)



```
root@kali:~# adduser hacking
Adding user `hacking' ...
Adding new group `hacking' (1001) ...
Adding new user `hacking' (1000) with group `hacking' ...
The home directory `/home/hacking' already exists.  Not copying from `/etc/skel'
.
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for hacking
Enter the new value, or press ENTER for the default
	Full Name []:
	Room Number []:
	Work Phone []:
	Home Phone []:
	Other []:
Is the information correct? [Y/n] Y
root@kali:~# cat /etc/shadow
```

So, first we actually tried to add a user and for this particular user, we try to keep a very small name which is very easily determinable directly from the dictionary right. So, after giving all the details of the user including the password and if at all we want to give any specific details, we verify that the information is correct and then ask the next to proceed further.

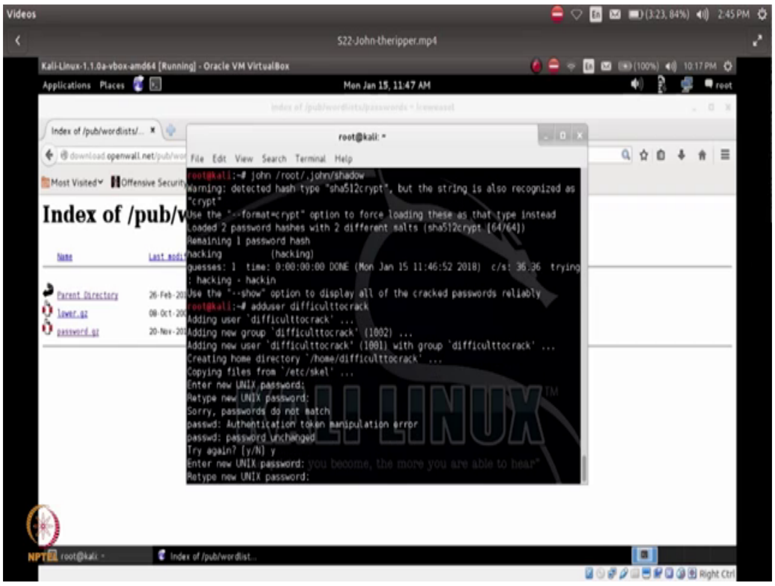
(Refer Slide Time: 08:43)



```
ntp:*:16497:0:99999:7:::
Debian-exim:!:16497:0:99999:7:::
arpwatch:!:16497:0:99999:7:::
avahi:*:16497:0:99999:7:::
beef-xss:*:16497:0:99999:7:::
dradis:*:16497:0:99999:7:::
pulse:*:16497:0:99999:7:::
speech-dispatcher:!:16497:0:99999:7:::
haldaemon:*:16497:0:99999:7:::
sshd:*:16497:0:99999:7:::
snmp:*:16497:0:99999:7:::
iodine:*:16497:0:99999:7:::
postgres:*:16497:0:99999:7:::
redsocks:!:16497:0:99999:7:::
stunnel4:!:16497:0:99999:7:::
statd:*:16497:0:99999:7:::
sslh:!:16497:0:99999:7:::
Debian-gdm:*:16497:0:99999:7:::
rtkit:*:16497:0:99999:7:::
saned:*:16497:0:99999:7:::
vboxadd:!:16507::::::
hacking:$6$NrIKnX4B$riu54G7bcw0h.PdtVfmwYDil9R7X0JaDyl6WZv23L1jdeWNU/HTjJ5kH0ngA
TK1FvGYHXhdQbcM.G7IrTjtN1:17546:0:99999:7:::
root@kali:~#
```

Now, if you see the shadow file in which this particular detail will actually be getting created, you find that this particular word user called hacking is created here as last entry in it, and it also has a huge encrypted string or a crypted string let us say for that particular user name as part of the shadow file.

(Refer Slide Time: 09:09)



```
root@kali:~# john /root/.john/shadow
Warning: detected hash type "sha512crypt", but the string is also recognized as
"crypt"
Use the "--format=crypt" option to force loading these as that type instead
Loaded 2 password hashes with 2 different salts (sha512crypt [64/64])
Remaining 1 password hash
hacking          (hacking)
guesses: 1  time: 0:00:00:00 DONE (Mon Jan 15 11:46:52 2018)  c/s: 36.36  trying
: hacking - hackin
Use the "--show" option to display all of the cracked passwords reliably
root@kali:~# adduser difficulttocrack
Adding user `difficulttocrack' ...
Adding new group `difficulttocrack' (1002) ...
Adding new user `difficulttocrack' (1001) with group `difficulttocrack' ...
Creating home directory `/home/difficulttocrack' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
Sorry, passwords do not match
passwd: Authentication token manipulation error
passwd: password unchanged
Try again? [y/N] y
Enter new UNIX password:
Retype new UNIX password:
```

So, what we do then is, we basically copying this shadow file into directory where the john the ripper tool is basically going to be making use of as its configuration directory right.

So, you have a directory called dot john under slash root, which is basically what it is going to be making uses of the configuration directory with with in which it expects the the the these files to be present right. So, we going to copy that there and then we are now going to run the tool john. So, that is basically how in the command line, we run the tool we run this john the ripper tool and then we now specify what is it that we want to really find out here. So, if you really find out what is it that it is actually done it has try to find out what kind of message digest algorithm is being made use of, and then look at it here it now prints this thing the username, and I had actually given the password is hacking right.

So, that has also printed the password as hacking right. So, this is basically the password that I had specified for that user, when I had actually created the this particular user with the add user command right. Now if you actually tried to create a new user with a very difficult password right. So, we are now creating a user called difficult to crack. So, that is the username and I have actually given it a very very long password with alphan

alphan numeric numbers, then punctuation symbols and so on right. So, it take so much time for even meet for me to type even the password string here. So, we can also see here that because of the long string I had actually made some mistakes while entering the password verification.

So, it has asked us to type password again right. So, this time it basically goes ahead an updates a password successfully, and then asking us to enter the optional details, it has now accepted the user creation. So, again we basically go ahead and copy the etc shadow file, because this particular newly created user is going to be actually have added right now should have got added into the shadow file.

So, we are basically re copying the shadow file into the johns john the ripper tools configuration directly, which is slashroot slashdot john right. And then re running the same command again if you see here it is actually telling again what is the the hash algorithm that has been actually made use of and for every key that I am pressing in the keyboard, it is telling me what are the different combinations that has actually been tried till now right and it is finding it very very difficult to determine that password right now, because this password which has been formed is a very very long string of around 20 22 characters with alphanumeric characters with alphabets with punctuation symbols and all the combinations put together right.

So, because of which now; it is actually been aborted by pressing the control c right now. So, this was basically a demonstration to tell you that, if you actually try to have a very simple password that is easily available in the dictionary, the tool helps to basically find out the password and crack the password very easily. But the movement as some of the portals today basically forces you keep a very long string with different kind of permutations and combinations in it you find the tool even though it has actually taken so, much time to run, it has not been successful in actually finding out the password even after this time right.

So, maybe if I actually give it a few hours of run, it might find out the password again depending on how cryptically I have set the password, but that is again a very secure mechanism of ensuring that you you cannot have your password busted very easily right. So, if you go to the open wall dot net this is basically the place where the john the ripper tool is actually available you also have standard password that is actually available here as part of their website which you could also download.

So, if you see for example, password dot gz this is actually a compressed file g zip file that is present which you can download do g unzip perfect and then use that also as the initial wordlist file for trying to crack the password on that particular system, which you are trying to target right now for cracking the password.

So, with this tool hopefully you actually have understood how as a very very basic mechanism this particular tool actually works, but I would also like to point out here that that are more sophisticated ways of actually using this tool, and I would very strongly recommend that you tried to play around with this and understand the different features that is there because this tool is something which is very very handy for a penetration tester, who is actually having penetration testing as a as a profession right. So, I would very strongly recommend that, this tool is actually practiced as much as possible.

Thank you.