BREAKING PASSWORDS

OBJECTIVE

The objective of this report is to showcase the procedure and different methods inolved in password cracking.

Password cracking is the process of using an application program to identify an unknown or forgotten password to a computer or network resource. It can also be used to help a threat actor obtain unauthorized access to resources.

With the information malicious actors gain using password cracking, they can undertake a range of criminal activities. Those include stealing banking credentials or using the information for identity theft and fraud.

TOOLS

The tool used in this report is pwdump. pwdump is the name of various Windows programs that outputs the LM and NTLM password hashes of local user accounts from the Security Account Manager (SAM) database and from the Active Directory domain's users cache on the operating system.

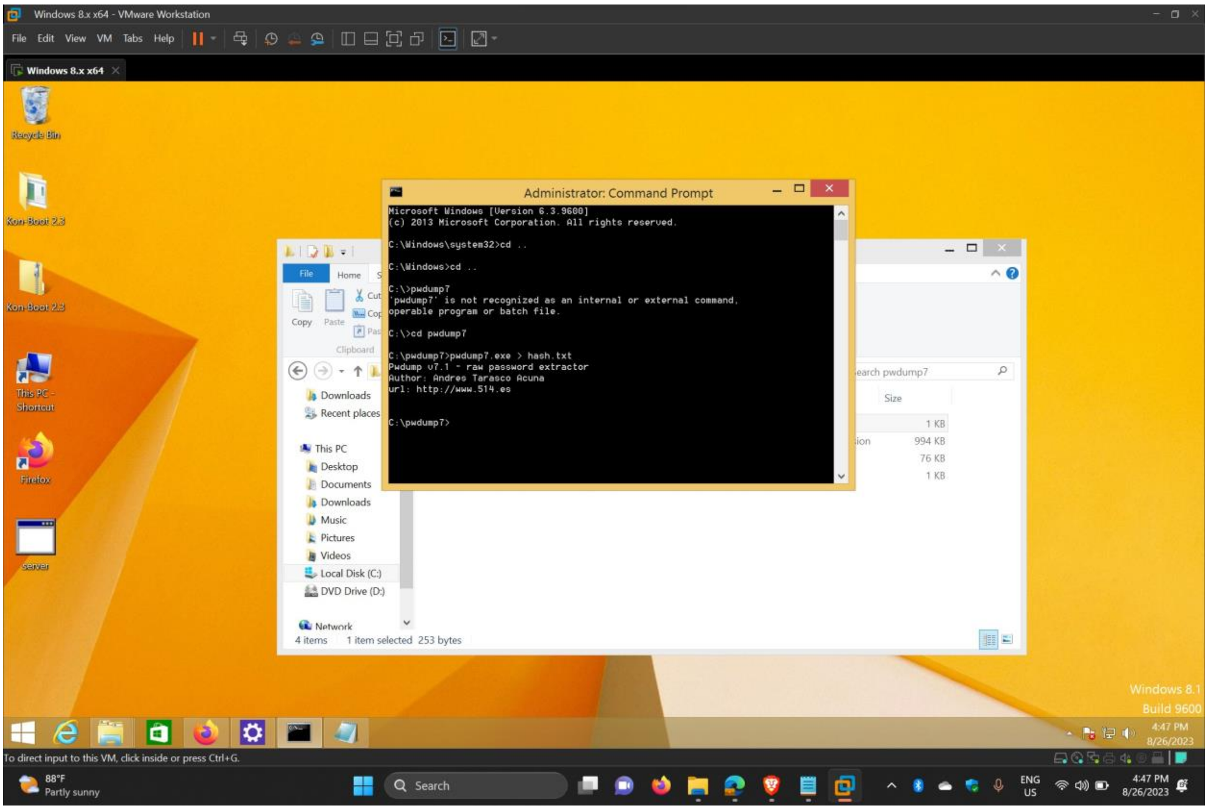
It is widely used, to perform both the famous pass-the-hash attack, or also can be used to brute-force user’s password directly. In order to work, it must be run under an Administrator account, or be able to access an Administrator account on the computer where the hashes are to be dumped. Pwdump could be said to compromise security because it could allow a malicious administrator to access user's passwords.

METHODOLOGY

The steps involved are:

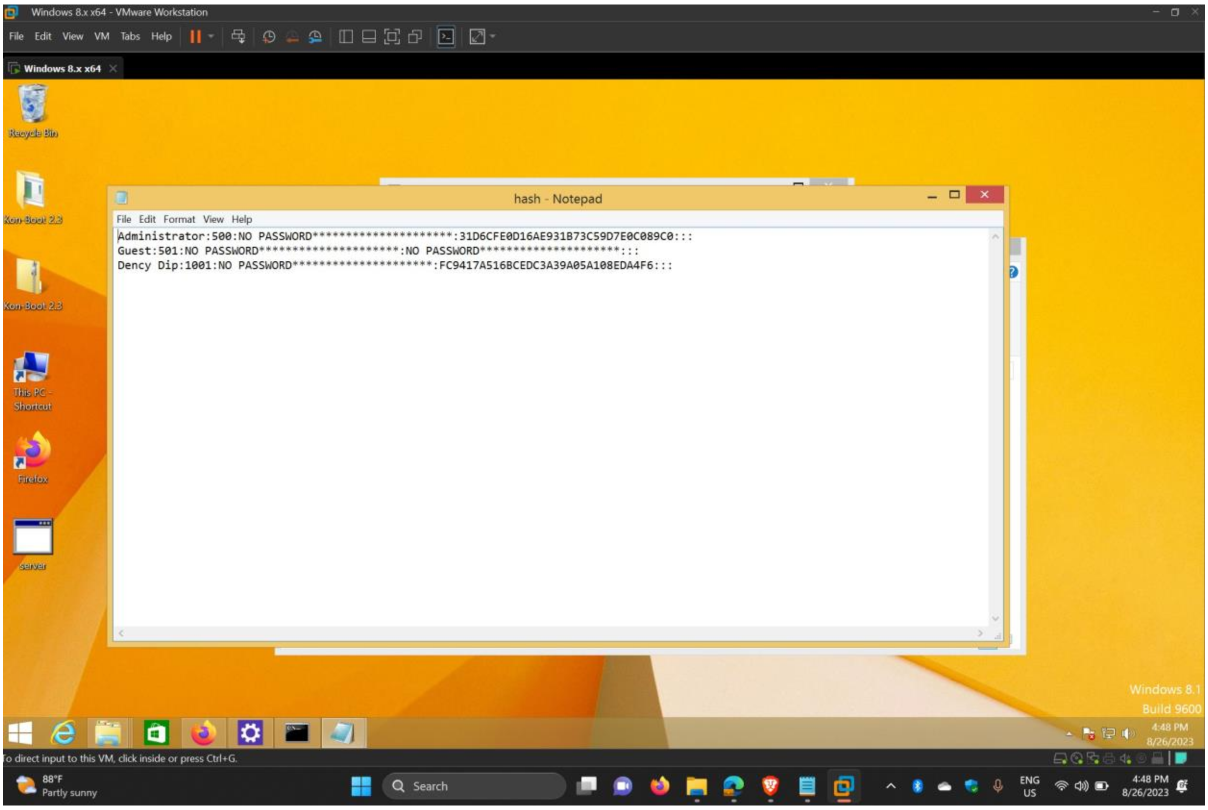
1. Go to openwall.com and download pwdump7 zip
2. Extract the zip file to C drive
3. Then execute the commands and then open the hash.txt file
4. Copy the hexadecimal number on the line of victim’s account name
5. Finally, go to crackstation and crack the hash to get the password of victim’s account.

PROOF OF CONCEPT



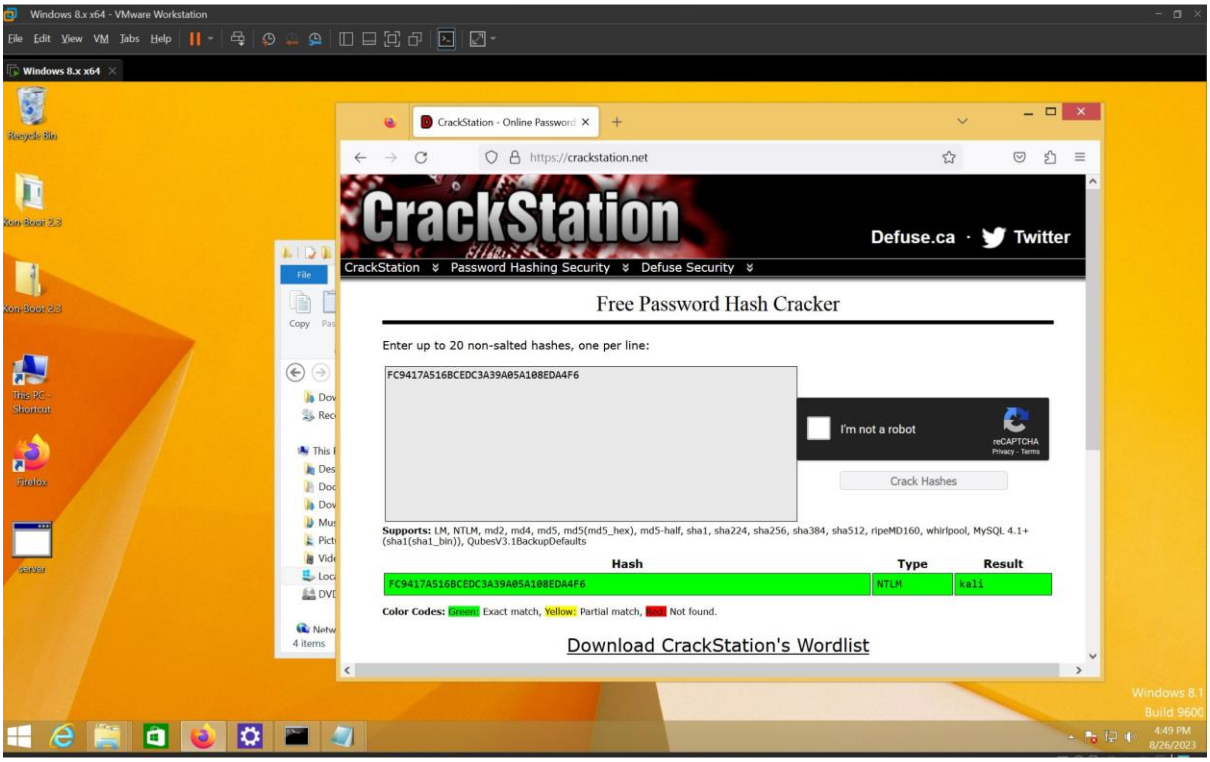
Windows 8.x x64 - VMware Workstation
File Edit View VM Tabs Help
Administrator: Command Prompt
Downloads
Recent places
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
DVD Drive (D:)
Network
4 items 1 item selected 253 bytes
Windows 8.1
Build 9600
To direct input to this VM, click inside or press Ctrl+G.

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd ..

C:\Windows>cd ..

C:\>pwdump7
'pwdump7' is not recognized as an internal or external command,
operable program or batch file.

C:\>cd pwdump7

C:\pwdump7>pwdump7.exe > hash.txt
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es


C:\pwdump7>
```



Windows 8.x x64 - VMware Workstation
File Edit View VM Tabs Help
hash - Notepad
File Edit Format View Help
Windows 8.1
Build 9600
To direct input to this VM, click inside or press Ctrl+G.

```
Administrator:500:NO PASSWORD*********************:31D6CFE0D16AE931B73C59D7E0C089C0:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
Dency Dip:1001:NO PASSWORD*********************:FC9417A516BCEDC3A39A05A108EDA4F6:::
```



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
FC9417A516BCEDC3A39A05A108EDA4F6
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
FC9417A516BCEDC3A39A05A108EDA4F6	NTLM	kali

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

CONCLUSION

Password cracking is the art of recovering stored or transmitted password. Password strength is determined by length, complexity, and unpredictability of a password value.