HACKTHEBOX

#HACKING101

PENTESTING TOOLS

TO USE IN AN AD ENVIRONMENT

CRACKMAPEXEC

CrackMapExec is an awesome **post-exploitation tool** that can be used for a multitude of reasons. **Password spraying, remote command execution**, or **running scripts**, CrackMapExec can do it all.

Plus, it is **OPSEC** (Operational security) **safe**, so you probably do not have to worry about getting detected.

01.

BLOODHOUND

Another amazing tool that can be used to gain information when you land in an unknown network is Bloodhound! Bloodhound can be used to **map the network** and **find complex attack paths** safely.

To avoid detection, try running everything in memory and exclude the Domain Controllers when collecting data.

02.

HACKTHEBOX

MIMIKATZ

The definitive pentesting tool for AD environments!

Mimikatz targets the way **Windows systems store credentials** in memory, and once you have debug privileges on a target machine, you can **extract hashes** of all the users that have logged into the machine (and even plaintext passwords for older systems).

03.

HACKTHEBOX

WHAT IS YOUR FAVORITE TOOL FOR AD PENTESTING?

Tell us in the comments

↓

PENTESTING TOOLS
TO USE IN AN AD ENVIRONMENT

#HACKING101