**Roles and Services**

Services on a particular host may serve the host itself or other hosts on the target network. It is necessary to create a profile of each targeted host, documenting the configuration of these services, their purpose, and how we can potentially use them to achieve our assessment goals. Typical server roles and services include:

* File and Print Servers
* Web and Database Servers
* Certificate Authority Servers
* Source Code Management Servers
* Backup Servers

Let's take Backup Servers as an example, and how, if we compromise a server or host with a backup system, we can compromise the network.

**Attacking Backup Servers**

In information technology, a backup or data backup is a copy of computer data taken and stored elsewhere so that it may be used to restore the original after a data loss event. Backups can be used to recover data after a loss due to data deletion or corruption or to recover data from an earlier time. Backups provide a simple form of disaster recovery. Some backup systems can reconstitute a computer system or other complex configurations, such as an Active Directory server or database server.

Typically backup systems need an account to connect to the target machine and perform the backup. Most companies require that backup accounts have local administrative privileges on the target machine to access all its files and services.

If we gain access to a backup system, we may be able to review backups, search for interesting hosts and restore the data we want.

As we previously discussed, we are looking for information that can help us move laterally in the network or escalate our privileges. Let's use [restic](https://restic.net/) as an example. Restic is a modern backup program that can back up files in Linux, BSD, Mac, and Windows.

To start working with restic, we must create a repository (the directory where backups will be stored). Restic checks if the environment variable RESTIC\_PASSWORD is set and uses its content as the password for the repository. If this variable is not set, it will ask for the password to initialize the repository and for any other operation in this repository.

We will use restic 0.13.1 and back up the repository C:\xampp\htdocs\webapp in E:\restic\ directory. To download the latest version of restic, visit <https://github.com/restic/restic/releases/latest>. On our target machine, restic is located at C:\Windows\System32\restic.exe.

We first need to create and initialize the location where our backup will be saved, called the repository.

**restic - Initialize Backup Directory**

restic - Initialize Backup Directory

PS C:\htb> mkdir E:\restic2; restic.exe -r E:\restic2 init

Directory: E:\

Mode LastWriteTime Length Name

---- ------------- ------ ----

d----- 8/9/2022 2:16 PM restic2

enter password for new repository:

enter password again:

created restic repository fdb2e6dd1d at E:\restic2

Please note that knowledge of your password is required to access

the repository. Losing your password means that your data is

irrecoverably lost.

Then we can create our first backup.

**restic - Back up a Directory**

restic - Back up a Directory

PS C:\htb> $env:RESTIC\_PASSWORD = 'Password'

PS C:\htb> restic.exe -r E:\restic2\ backup C:\SampleFolder

repository fdb2e6dd opened successfully, password is correct

created new cache in C:\Users\jeff\AppData\Local\restic

no parent snapshot found, will read all files

Files: 1 new, 0 changed, 0 unmodified

Dirs: 2 new, 0 changed, 0 unmodified

Added to the repo: 927 B

processed 1 files, 22 B in 0:00

snapshot 9971e881 saved

If we want to back up a directory such as C:\Windows, which has some files actively used by the operating system, we can use the option --use-fs-snapshot to create a VSS (Volume Shadow Copy) to perform the backup.

**restic - Back up a Directory with VSS**

restic - Back up a Directory with VSS

PS C:\htb> restic.exe -r E:\restic2\ backup C:\Windows\System32\config --use-fs-snapshot

repository fdb2e6dd opened successfully, password is correct

no parent snapshot found, will read all files

creating VSS snapshot for [c:\]

successfully created snapshot for [c:\]

error: Open: open \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\config: Access is denied.

Files: 0 new, 0 changed, 0 unmodified

Dirs: 3 new, 0 changed, 0 unmodified

Added to the repo: 914 B

processed 0 files, 0 B in 0:02

snapshot b0b6f4bb saved

Warning: at least one source file could not be read

**Note:** If the user doesn't have the rights to access or copy the content of a directory, we may get an Access denied message. The backup will be created, but no content will be found.

We can also check which backups are saved in the repository using the shapshot command.

**restic - Check Backups Saved in a Repository**

restic - Check Backups Saved in a Repository

PS C:\htb> restic.exe -r E:\restic2\ snapshots

repository fdb2e6dd opened successfully, password is correct

ID Time Host Tags Paths

--------------------------------------------------------------------------------------

9971e881 2022-08-09 14:18:59 PILLAGING-WIN01 C:\SampleFolder

b0b6f4bb 2022-08-09 14:19:41 PILLAGING-WIN01 C:\Windows\System32\config

afba3e9c 2022-08-09 14:35:25 PILLAGING-WIN01 C:\Users\jeff\Documents

--------------------------------------------------------------------------------------

3 snapshots

We can restore a backup using the ID.

**restic - Restore a Backup with ID**

restic - Restore a Backup with ID

PS C:\htb> restic.exe -r E:\restic2\ restore 9971e881 --target C:\Restore

repository fdb2e6dd opened successfully, password is correct

restoring <Snapshot 9971e881 of [C:\SampleFolder] at 2022-08-09 14:18:59.4715994 -0700 PDT by PILLAGING-WIN01\jeff@PILLAGING-WIN01> to C:\Restore

If we navigate to C:\Restore, we will find the directory structure where the backup was taken. To get to the SampleFolder directory, we need to navigate to C:\Restore\C\SampleFolder.

We need to understand our targets and what kind of information we are looking for. If we find a backup for a Linux machine, we may want to check files like /etc/shadow to crack users' credentials, web configuration files, .ssh directories to look for SSH keys, etc.

If we are targeting a Windows backup, we may want to look for the SAM & SYSTEM hive to extract local account hashes. We can also identify web application directories and common files where credentials or sensitive information is stored, such as web.config files. Our goal is to look for any interesting files that can help us archive our goal.

**Note:** restic works similarly in Linux. If we don't know where restic snapshots are saved, we can look in the file system for a directory named snapshots. Keep in mind that the environment variable may not be set. If that's the case, we will need to provide a password to restore the files.

Hundreds of applications and methods exist to perform backups, and we cannot detail each. This restic case is an example of how a backup application could work. Other systems will manage a centralized console and special repositories to save the backup information and execute the backup tasks.

As we move forward, we will find different backup systems, and we recommend taking the time to understand how they work so that we can eventually abuse their functions for our purpose.