Resources

https://securityonline.info/adrecon-active-directory-gathering-information-tool/

https://github.com/sense-of-security/ADRecon/blob/master/ADRecon.ps1

ADRecon: Active Directory Recon

ADRecon is a tool which extracts and combines various artifacts (as highlighted below) out of an AD environment. The information can be presented in a specially formatted Microsoft Excel report that includes summary views with metrics to facilitate analysis and provide a holistic picture of the current state of the target AD environment.

The tool is used by various classes of security professionals like auditors, DFIR, students, administrators, etc. It can also be an invaluable post-exploitation tool for a penetration tester.

It can be run from any workstation that is connected to the environment, even hosts that are not domain members. Furthermore, the tool can be executed in the context of a non-privileged (i.e. standard domain user) account. Fine-Grained Password Policy, LAPS, and BitLocker may require Privileged user accounts. The tool will use Microsoft Remote Server Administration Tools (RSAT) if available, otherwise, it will communicate with the Domain Controller using LDAP.

The following information is gathered by the tool:

- Forest;
- Domain;
- Trusts;
- Sites;
- Subnets;
- Default Password Policy;
- Fine-Grained Password Policy (if implemented);
- Domain Controllers, SMB versions, whether SMB Signing is supported and FSMO roles;
- Users and their attributes;
- Service Principal Names (SPNs);
- Groups and memberships;
- Organizational Units (OUs);

- ACLs for the Domain, OUs, Root Containers and GroupPolicy objects;
- Group Policy Object details;
- DNS Zones and Records;
- Printers;
- Computers and their attributes;
- LAPS passwords (if implemented);
- BitLocker Recovery Keys (if implemented); and
- GPOReport (requires RSAT).
- Kerberoast (not included in the default collection method).