

91.1 - Ldapdomaindump - Domain Enumeration

We have used this tool before. We used to perform the IPv6 Relay Attack.

If IPv6 is not possible in the network, this tool will help us with other attacks.

To run this tool in such scenario, we can run this tool as follows:

1 - Create a directory

2 - cd into it

3 - Run: "#sudo ldapdomaindump ldaps://DC_IP -u "ONEPIECE\LMonkey" -p Password1" If we want to output to a specific folder we can use "-o PATH/TO/DIR". if we omit the flag, it will save to the current pwd.

```
(kali@kali)~[~/Desktop/TCM-ActiveDirectory-Lab/ldapdomaindump/onepiece.local]
$ sudo ldapdomaindump ldaps://192.168.163.156 -u "ONEPIECE\LMonkey" -p Password1

[*] Connecting to host...
[*] Binding to host
Traceback (most recent call last):
  File "/usr/local/bin/ldapdomaindump", line 3, in <module>
    ldapdomaindump.main()
  File "/usr/local/lib/python2.7/dist-packages/ldapdomaindump/__init__.py", line 940, in main
    if not c.bind():
  File "/usr/local/lib/python2.7/dist-packages/ldap3/core/connection.py", line 563, in bind
    response = self.do_ntlm_bind(controls)
  File "/usr/local/lib/python2.7/dist-packages/ldap3/core/connection.py", line 1302, in do_ntlm_bind
    request = bind_operation(self.version, 'SICILY_RESPONSE_NTLM', ntlm_client, result['server_creds'])
  File "/usr/local/lib/python2.7/dist-packages/ldap3/operation/bind.py", line 81, in bind_operation
    server_creds = name.create_authenticate_message()
  File "/usr/local/lib/python2.7/dist-packages/ldap3/utils/ntlm.py", line 379, in create_authenticate_message
    nt_challenge_response = self.compute_nt_response()
  File "/usr/local/lib/python2.7/dist-packages/ldap3/utils/ntlm.py", line 485, in compute_nt_response
    response_key_nt = self.ntowf_v2()
  File "/usr/local/lib/python2.7/dist-packages/ldap3/utils/ntlm.py", line 496, in ntowf_v2
    password_digest = hashlib.new('MD4', self._password.encode('utf-16-le')).digest()
  File "/usr/lib/python2.7/hashlib.py", line 116, in __new
    return __get_builtin_constructor(name)(string)
  File "/usr/lib/python2.7/hashlib.py", line 97, in __get_builtin_constructor
    raise ValueError('unsupported hash type ' + name)
ValueError: unsupported hash type MD4
```

Advised to use the absolute path of the command software.

```
(kali@kali)~[~/Desktop/TCM-ActiveDirectory-Lab/ldapdomaindump/onepiece.local]
$ sudo /usr/bin/ldapdomaindump ldaps://192.168.163.156 -u "ONEPIECE\LMonkey" -p Password1
[sudo] password for kali:
[*] Connecting to host...
[*] Binding to host
[*] Bind OK
[*] Starting domain dump
[*] Domain dump finished

(kali@kali)~[~/Desktop/TCM-ActiveDirectory-Lab/ldapdomaindump/onepiece.local]
$ ls
domain_computers_by_os.html  domain_computers.html  domain_groups.grep  domain_groups.json  domain_policy.html  domain_trusts.grep  domain_trusts.json  domain_users.grep  domain_users.json
domain_computers.grep      domain_computers.json  domain_groups.html  domain_policy.grep  domain_policy.json  domain_trusts.html  domain_users_by_group.html  domain_users.html
```

It worked!

This is all very good information. Here, we can see the that password of the service Admin account we created, and left in the description is picked up by the ldapdomaindump.

file:///home/kali/Desktop/TCM-ActiveDirectory-Lab/ldapdomaindump/onepiece.local/domain_users_by_group.html									
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Netcat Shell Stabilizati...									
Domain Users									
CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
gDKjEqGfSI	gDKjEqGfSI	gDKjEqGfSI	10/06/24 22:32:06	10/06/24 22:32:06	01/01/01 00:00:00	NORMAL_ACCOUNT	10/06/24 22:32:06	1109	
Zoro Roronoa	Zoro Roronoa	ZRoronoa	09/29/24 00:35:20	10/21/24 02:44:33	10/21/24 23:49:41	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	09/29/24 00:35:20	1106	
Luffy Monkey	Luffy Monkey	LMonkey	09/29/24 00:32:09	10/31/24 00:03:54	10/31/24 00:03:54	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	09/29/24 00:32:09	1105	
SQL Service	SQL Service	SQLService	09/29/24 00:00:59	09/29/24 00:46:53	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	09/29/24 00:00:59	1104	The password is Mypassword123#
Usopp Sogeking	Usopp Sogeking	USogeking	09/28/24 23:55:46	09/29/24 19:18:36	10/11/24 01:56:14	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	09/28/24 23:55:47	1103	
krbtgt	krbtgt	krbtgt	09/28/24 02:05:52	09/28/24 02:21:02	01/01/01 00:00:00	ACCOUNT_DISABLED, NORMAL_ACCOUNT	09/28/24 02:05:52	502	Key Distribution Center Service Account
Administrator	Administrator	Administrator	09/28/24 02:05:11	10/31/24 00:04:36	10/31/24 00:04:36	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	09/28/24 00:12:11	500	Built-in account for administering the computer/domain
Group Policy Creator Owners									
CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
SQL Service	SQL Service	SQLService	09/29/24 00:00:59	09/29/24 00:46:53	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	09/29/24 00:00:59	1104	The password is Mypassword123#
Usopp Sogeking	Usopp Sogeking	USogeking	09/28/24 23:55:46	09/29/24 19:18:36	10/11/24 01:56:14	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	09/28/24 23:55:47	1103	
Administrator	Administrator	Administrator	09/28/24 02:05:11	10/31/24 00:04:36	10/31/24 00:04:36	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	09/28/24 00:12:11	500	Built-in account for administering the computer/domain
Domain Admins									
CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
SQL Service	SQL Service	SQLService	09/29/24 00:00:59	09/29/24 00:46:53	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	09/29/24 00:00:59	1104	The password is Mypassword123#
Usopp Sogeking	Usopp Sogeking	USogeking	09/28/24 23:55:46	09/29/24 19:18:36	10/11/24 01:56:14	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	09/28/24 23:55:47	1103	
Administrator	Administrator	Administrator	09/28/24 02:05:11	10/31/24 00:04:36	10/31/24 00:04:36	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	09/28/24 00:12:11	500	Built-in account for administering the computer/domain
Enterprise Admins									

Obviously we are looking for low hanging fruits first. We are looking for domain admin accounts, if account is expired or not, domain users, and much more. All information coming from the dump is going to be valuable.

And this is one method to enumerate Active Directory Domain.