From Pass-the-Hash to Pass-the-Ticket with No Pain

Posted: Jan 25, 2017 by **Andrea Pierini**

Share

We are all grateful to the Microsoft which gave us the possibility to use the "Pass the Hash" technique to share if we have the NTLM hashes of the user password, we can authenticate against the remote system without knowing the real password, just using the hashes.

Things were (finally) changing, starting from Windows 7, Microsoft tried to "patch" this vulnerability introducing Kerberos authentication, as explained here: https://www.hackingarticles.in/wp-content/uploads/2016/06/Pass-the-Hash-is-dead-long-live-Kerberos-Journey-to-Kerberos-Hell.jpg-scaled.jpg

Get free, expert instruction from anywhere!
Enroll in an upcoming live online boot camp and earn your certification, guaranteed!
Get Pricing

But with the advent of Windows 2012R2 and the corresponding Domain Functional Level, it is possible to completely prohibit the NTLM authentication and consequently PTH for domain users belonging to the special group "Protected Users Group".

Sure, with a manipulator session we could easily bust the "encryption" module and impersonate the domain admin user who just logged in by "stealing" the Kerberos ticket.

And with this appropriate shell start our lateral movement.

But what if we can't use Mimikatz/pt or similar tools because the Antivirus is blocking us?

Game over? No! We have the Kerberos Authentication in play. Instead of pressing the hash, we will pass the ticket!

Imagine this scenario:

- We have a remote shell reverse or bind, for example, PowerShell - with Local System privileges obtained on an MSSQL server through sp_cmdshell via sqlinjection.

With our obfuscated ps1 version of Invoke-Mimi we can't crack the clear text passwords of the logged domain administrator given that we have to face with a Windows 2012 Server:

```
PS C:\windows\system32 > whoami /groups /fo list

GROUP INFORMATION
-----------------

Group name:  Everyone
Type:        Well-known group
SID:         S-1-1-0
Attributes:  Mandatory group, Enabled by default, Enabled group

Group name:  BUILTIN\Users
Type:        Alias
SID:         S-1-5-32-545
Attributes:  Mandatory group, Enabled by default, Enabled group

Group name:  BUILTIN\Administrators
Type:        Alias
SID:         S-1-5-32-544
Attributes:  Mandatory group, Enabled by default, Enabled group, Group owner

Group name:  NT AUTHORITY\NTLM Authentication
Type:        Well-known group
SID:         S-1-5-64-10
Attributes:  Mandatory group, Enabled by default, Enabled group

Group name:  Mandatory Label\Medium Mandatory Level
Type:        Label
SID:         S-1-16-8192
Attributes:  Mandatory group, Enabled by default, Enabled group, Integrity level
```

Stay Updated
Get exclusive offers and updates straight to your inbox.
Email Address
SUBSCRIBE
© 2025 Vintage Wine Cellar
Privacy Policy
Wine Cellar Cooling Units
Wine Cellar Cooling Units
Wine Cellar Cooling Units