

N00PY BLOG

/Users/n00py/

HOME DEFENSE GITHUB LINKEDIN OSX PENTESTING RESEARCH WALKTHROUGHS WHOAMI

Home / Pentesting / Resetting Expired Passwords Remotely

Resetting Expired Passwords Remotely

📅 September 22, 2021 👤 n00py 📁 Pentesting 💬 0 Comment

I've often found that while performing password guessing on a network, I'll find valid credentials, but the password will be expired. This presents a challenge, because the credentials are of limited use until they are reset.

```
1 # crackmapexec smb 10.0.0.15 -u locked -p Password1
2 SMB 10.0.0.15 445 WIN-NDA9607EHKS [*] Windows 10.0 Buil
3 SMB 10.0.0.15 445 WIN-NDA9607EHKS [-] n00py.local\locke
4
5 # crackmapexec smb 10.0.0.15 -u expired -p Password1
6 SMB 10.0.0.15 445 WIN-NDA9607EHKS [*] Windows 10.0 Buil
7 SMB 10.0.0.15 445 WIN-NDA9607EHKS [-] n00py.local\expir
```

Throughout my testing I've found multiple ways to reset the passwords, however each contain some caveats.

I've tested using an account that has an expired password (STATUS_PASSWORD_EXPIRED) as well as an account that has the "User must change password at next logon" box checked (STATUS_PASSWORD_MUST_CHANGE). I've named them "expired" and "locked" respectively.

Please ignore my poor naming, as the "locked" account is **NOT** disabled (STATUS_ACCOUNT_DISABLED) or locked (STATUS_ACCOUNT_LOCKED_OUT), and the "expired" account is **NOT** expired (STATUS_ACCOUNT_EXPIRED), only the password is. As far as I know there is no possible way to unset those without admin.

See the original Twitter thread here:

Doing a password spray and hit valid creds but get STATUS_PASSWORD_MUST_CHANGE? Have no fear. Look for "Terminal Services Doesn't Use NLA" in Nessus output or use the rdp-enum-encryption nmap script to look for RDP that supports Native RDP/ SSL. (1/3) pic.twitter.com/iXjbKQQDcY — n00py (@n00py1) September 16, 2021

Outlook Web Access

Caveats: Requires Outlook Web Access to be accessible

This is a very reliable way to reset a password, however you of course need to find an exposed Outlook Web Access application. It will typically look for something like this at *mail.DOMAIN.TLD* or *HOSTNAME/OWA/*.

Search ...



CATEGORIES

Select Category



N00PY BLOG

Resetting Expired Passwords Remotely

Dumping Plaintext RDP credentials from svchost.exe

The Dangers of Endpoint Discovery in VIPRE Endpoint Security

Dumping LAPS Passwords from Linux

Alternative ways to Pass the Hash (PtH)

Password Spraying Secure Logon for F5 Networks

Extracting files from Burp Intruder Output

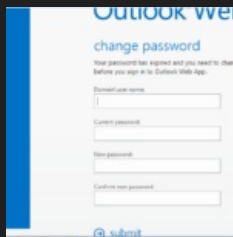
Exploiting LDAP Server NULL Bind

Managing Active Directory groups from Linux

Zero day vulnerabilities in Determine Selectica Contract Lifecycle Management (SCLM) v5.4

September 2021

M	T	W	T	F	S	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19



When you find one it's simply a matter of entering the credentials and a change password screen will pop up.

Remote Desktop Protocol

Caveats: Requires RDP without NLA enforced

This is the way I've been doing it a long time, and has been pretty reliable. The hard part is finding a system without NLA required. The good part however is that the user does not need permissions to RDP to the system. You can still reset the password regardless.

If you have completed a Nessus scan, look for the finding "Terminal Services Doesn't Use Network Level Authentication (NLA) Only".

Anything that shows up there will work. you can also use nmap:

```
1 # nmap 10.0.0.2 -p 3389 --script rdp-enum-encryption
2
3 PORT STATE SERVICE
4 3389/tcp open  ms-wbt-server
5 | rdp-enum-encryption:
6 | Security layer
7 | CredSSP (NLA): SUCCESS
8 | CredSSP with Early User Auth: SUCCESS
9 | RDPSTLS: SUCCESS
10 | SSL: SUCCESS
11 | RDP Protocol Version: Unknown
12 | MAC Address: 00:0C:29:DE:EA:61 (VMware)
```

You will want to see the "SSL: SUCCESS" in the output.

You can also use **Metasploit** to find this information as well:

```
1 msf6 auxiliary(scanner/rdp/rdp_scanner) > run
2
3 [*] 10.0.0.2:3389 - Detected RDP on 10.0.0.2:3389 (Windows version: 10.0.
4 [*] 10.0.0.2:3389 - Scanned 1 of 1 hosts (100% complete)
5 [*] Auxiliary module execution completed
```

Use **rdesktop** to connect to the system without specifying any username or password. Type "yes" to trust the certificate.

```
1 # rdesktop 10.0.0.2
2
3 Do you trust this certificate (yes/no)? yes
4 Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
5 Core(warning): Certificate received from server is NOT trusted by this sy
6 Connection established using SSL.
```

From here you can reset the password, and can then return to your other command line tools.

smbpasswd

Caveats: Requires anonymous access to IPC\$ Share

smbpasswd probably the most simple way to perform a reset remotely, though it does have some conditions. To perform the reset, simply provide the remote host with the **-r** flag and the username with the **-U** flag.

```
1 smbpasswd -r 10.0.0.15 -U 'expired'
2 Old SMB password:
3 New SMB password:
```

20	21	22	23	24	25	26
27	28	29	30			

« May

ARCHIVES

September 2021

May 2021

December 2020

August 2020

May 2020

February 2020

January 2020

December 2019

June 2019

March 2019

October 2018

August 2018

June 2018

April 2018

March 2018

January 2018

December 2017

November 2017

October 2017

September 2017

August 2017

June 2017

April 2017

March 2017

January 2017

October 2016

Follow @n00py1 8,028 followers

Tweets by @n00py1

n00py Retweeted

Mike Felch
@ustayready

@424f424f and I dropped some new initial access TTP's for your red team engagement at @WWHackinFest. You can leverage RDP files to bypass email attachment blocklists to plant C2 binaries, exfil data & steal clipboards.. or just phish Azure tokens! #wwhf slideshare.net/MichaelFelch/s...

SlideShare @SlideShare

```

4 Retype new SMB password:
5
6 Password changed for user expired on 10.0.0.15.
7
8 # smbpasswd -r 10.0.0.15 -U 'locked'
9 Old SMB password:
10 New SMB password:
11 Retype new SMB password:
12 Password changed for user locked on 10.0.0.15.

```

A review of the packet capture shows what happens; it first tried to authenticate with the account, gets the "password expired" message, and then connects anonymously to the IPC\$ share. From there it is able to perform the password reset.

By default, anyone can connect over IPC\$ anonymously. It is sometimes the case however that IPC\$ is not accessible; and in this case this will not work. Below is smbpasswd with the debug flag set. As you can see it fails when trying to establish the NULL session.

I'd still always recommend trying this method first, but if you ever find that it does not work it may be because of the NULL session limitation.

ChangePwd

Caveats: Requires access to IPC\$ Share and Windows

This is a pretty old utility for Windows that has been around since 1999. You can [download it here](#). Despite its age, it works flawlessly and does not need any admin permissions to run.

A packet capture reveals that it works in much the same way as smbpasswd, in regards to the connection to IPC\$. Notable however, if that it does not perform an anonymous connection, it connects to IPC\$ with the current logged in user. In this case, even if IPC\$ was limited for NULL sessions it can still perform the reset as long as you have at least one other user.

Impacket smbpasswd

Caveats: Requires ~~anonymous~~ access to IPC\$ Share

This is basically the same as smbpasswd, but re-implemented in a non-interactive way in Impacket by [snowcrash](#). [Blog post here](#).

At the time of writing, his latest version (non-merged) is [here](#).

```

1 # python3 smbpasswd.py locked:Password1@n00py.local -newpass Password2
2 Impacket v0.9.24.dev1+20210917.161743.0297480b - Copyright 2021 SecureAut
3
4 [!] Password is expired, trying to bind with a null session.
5 [*] Password was changed successfully.

```

A review of the network traffic found that this was pretty much the same as the original smbpasswd.

Testing has indicated that without anonymous access to IPC\$, this will also fail in the same way smbpasswd does.

Based on what I learned when looking at ChangePwd, it's actually still possible to do this without needing a NULL sessions, assuming you have any other valid user creds. I may add this to the Impacket smbpasswd.py someday, but for now you can do this just by modifying the line where it says:

```

1 if anonymous:
2     rpctransport.set_credentials(username='', password='', domain='', lmh

```

And just replacing the blank values with another set of valid creds.

SetADAccountPwd

Caveats: Requires Windows and RSAT tools

This method is also super easy, only hindered by the fact that you need RSAT tools. Sadly, you need



Sep 24, 2021

n00py Retweeted

Nick VanGilder
@nickvangilder

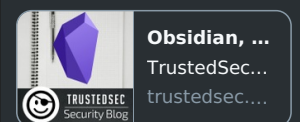
Undocumented method for proxied execution of an unsigned .NET assembly:
powershell.exe -command "set-location -path c:\windows\diagnostics\system\networking; import-module .\UtilityFunctions.ps1; RegSnapin ..\..\..\temp\unsigned.dll; [Program.Class]::Main()"

Sep 23, 2021

n00py Retweeted

TrustedSec
@TrustedSec

Our Targeted Operations team recently looked to improve their knowledge management strategy. [@L1NKD34D](#) provides a behind-the-scenes look at how Obsidian has been customized and evaluated as a solution. Bonus! It's available to as an open-source resource. hubs.la/H0WNgHR0



Sep 7, 2021

n00py
@n00py1

Replying to @n00py1
Notable tidbits: All Linux based remote methods require SMB Null sessions, but I found a way do it if you have any other valid creds.

Sep 22, 2021

n00py
@n00py1

Replying to @n00py1
[twitter.com/n00py1/status/...](https://twitter.com/n00py1/status/1438528686332973065)
<https://twitter.com/n00py1/status/1438528686332973065>

Sep 22, 2021

n00py

admin to install them on a Windows desktop.

If you do happen to have them installed, the [syntax](#) is super simple.

Powershell Script

Caveats: Requires access to IPC\$ Share and Windows

This method is great if you have access to Windows and don't want to install anything or drop binaries. I found [this script on StackExchange](#) and it works well:

```
1 function Set-PasswordRemotely {
2     [CmdletBinding()]
3     param(
4         [Parameter(Mandatory = $true)][string] $UserName,
5         [Parameter(Mandatory = $true)][string] $OldPassword,
6         [Parameter(Mandatory = $true)][string] $NewPassword,
7         [Parameter(Mandatory = $true)][alias('DC', 'Server', 'ComputerName')]
8     )
9     $DllImport = @'
10 [DllImport("netapi32.dll", CharSet = CharSet.Unicode)]
11 public static extern bool NetUserChangePassword(string domain, string user,
12 '0'
13 $NetApi32 = Add-Type -MemberDefinition $DllImport -Name 'NetApi32' -
14 if ($result = $NetApi32::NetUserChangePassword($DomainController, $User
15 Write-Output -InputObject 'Password change failed. Please try again.'
16 } else {
17 Write-Output -InputObject 'Password change succeeded.'
18 }
19 }
```

Original source is [here](#).

You can run it interactively or in one line.

```
1 PS C:\Users\n00py> Set-PasswordRemotely
2
3 cmdlet Set-PasswordRemotely at command pipeline position 1
4 Supply values for the following parameters:
5 UserName: locked
6 OldPassword: Password1
7 NewPassword: Password11
8 DomainController: n00py.local
9 Password change succeeded.
10
11 PS C:\Users\n00py> Set-PasswordRemotely locked Password1 Password12 n00py
12 Password change succeeded.
```

Rubeus

Caveats: Requires Windows / AV Evasion

A password change can also be performed with [Rubeus](#) using Kerberos magic. I'm not going to pretend to understand how this actually works, so I'll leave that to Harmj0y to explain in [his blog post](#).

To perform the change first get a ticket with the old password:

And then change the password using the ticket:

Now for the techniques I tried, but do not appear to work in any way.

File Explorer

Findings: Does not work / Not possible

I thought perhaps this may be possible to do in Explorer when connecting to a remote share. While it does at least give an informative error message, it does not allow any way to update the password.

**n00py**
@n00py1

I've written a blog about resetting expired passwords remotely, based on my Twitter thread earlier this week.

Thanks for everyone who commented and gave input![n00py.io/2021/09/reset t...](#)

**Resetting ...**
I've often f...
n00py.io

Sep 22, 2021

n00py Retweeted

**sneakerhax**
@sneakerhax

The Red Team @Adobe is looking to expand!

If you have questions let me know

Offensive Security Engineer / Red
Team[adobe.wd5.myworkdayj obs.com/en-US/external...](#)

Sep 22, 2021

n00py Retweeted

**Matt Eidelberg**
@Tyl0us

Check out @garrfoster article on PetitPotam & Active Directory Certificate Services @OptivSourceZero.
[optim.com/insights/sourc...#infosec #netsec](#)

**PetitPotam & Active ...**
Multiple CVEs involving...
[optim.com](#)

Aug 10, 2021

n00py Retweeted

**Rasta Mouse**
@_RastaMouse

[BLOG]
Short post on how to do NTLM relaying via Cobalt Strike using PortBender, WinDivert and ntlmrelayx.
[rastamouse.me/ntlm-relaying-...](#)

Jul 29, 2021

n00py Retweeted

**d3adc0de**

Kpasswd

Findings: Does not work / Not possible

I was hoping **kpasswd** would do the trick, however it simply gives you the message "Password Incorrect" with an expired password.

```
1 kpasswd locked@n00py.local
2 locked@n00py.local's Password:
3 kpasswd: Password incorrect
```

Kinit does at least give you the courtesy of telling you the password expired, but does not contain any mechanism to reset the password either.

```
1 kinit locked@n00py.local
2 locked@n00py.local's Password:
3 Password has expired
4 kinit: Password incorrect
```

LDAP

Findings: Does not work / Not possible

This is the one I REALLY wanted to work, but as far as I can tell it doesn't. Any attempt to bind with an expired password fails. I've seen multiple people (1,2) mention that this should be possible, but I had no luck with it. It is mentioned to change the password you need to use LDAPS, but as far as I can tell this is only relevant to changing the password and not the initial bind.

Below is my attempt to use ldap3 in Python to bind using an expired password. Note the response containing the 49 result with error 773 and 532 respectively.

```
1 # python3
2 >>> import ldap3
3 >>> from ldap3 import ALL, Server, Connection, NTLM, extend, SUBTREE
4 >>> server = ldap3.Server('n00py.local', get_info = ldap3.ALL)
5 >>> user = 'locked'
6 >>> password = 'Password1'
7 >>> c = Connection(server, "n00py\\" + user, password=password, authentic
8 >>> c.bind()
9 False
10 >>> c.result
11 {'result': 49, 'description': 'invalidCredentials', 'dn': '', 'message':
12
13 >>> user = 'expired'
14 >>> c = Connection(server, "n00py\\" + user, password=password, authentic
15 >>> c.bind()
16 False
17 >>> c.result
18 {'result': 49, 'description': 'invalidCredentials', 'dn': '', 'message':
```

Packet captures:

I also did retry it in Python ldap3 using LDAPS, but it gave the same result.

[Tweet](#)

[« PREVIOUS POST](#)

Leave a Reply

You must be [logged in](#) to post a comment.

[« PREVIOUS POST](#)

@KlezVirus

[github.com/klezVirus/CVE-...](https://github.com/klezVirus/CVE-2021-40444)
As the official patch has been released, I guessed it would be fine to release my version of [#CVE202140444](#). This was quite fun to play with, tbh. This generator works to load arbitrary DLLs, and give a decent description of the required CAB patches

klezVirus/CVE-2021-40444
CVE-2021-40444 - Fully Weaponized Microsoft Office Word RCE Exploit
Contributor Issues Stars Forks
GitHub - klezVirus/C...
CVE-2021-40444 - Fully...
github.com

Sep 16, 2021

n00py Retweeted

inversecos @inversecos

I built an attack matrix for [#Office365](#) of various techniques used by (mostly) [#APT](#) groups to bypass [#MFA](#), achieve persistence, impersonate users including ...

> Malicious App Registrations
> Abuse of Service Principals
> API Bruteforce
> Abuse of PTA
bit.ly/2XnKju3

OFFICE 365 ATTACK MATRIX				
Technique	Category	Impact	Tools	References
Malicious App Registrations	Abuse of Service Principals	Access to sensitive data	Powercat, Powercat, Powercat	https://www.microsoft.com/en-us/security/blog/2021/09/16/office-365-attack-matrix/
Abuse of Service Principals	Abuse of Service Principals	Access to sensitive data	Powercat, Powercat, Powercat	https://www.microsoft.com/en-us/security/blog/2021/09/16/office-365-attack-matrix/
API Bruteforce	Abuse of Service Principals	Access to sensitive data	Powercat, Powercat, Powercat	https://www.microsoft.com/en-us/security/blog/2021/09/16/office-365-attack-matrix/
Abuse of PTA	Abuse of Service Principals	Access to sensitive data	Powercat, Powercat, Powercat	https://www.microsoft.com/en-us/security/blog/2021/09/16/office-365-attack-matrix/

Sep 17, 2021



n00py Retweeted


Optiv Source Zero @OptivSourceZero

We've got a new tool for you. Check out [#Talon](#) by [@Tyl0us](#)! 😊 Talon is designed to perform automated [#Password](#) guessing attacks undetected. Talon can also enumerate users to identify valid users in a domain using Kerberos. [#InfoSec](#)
github.com/optiv/Talon


optiv/Talon
A password guessing tool that targets the Kerberos and LDAP services within the Windows Active Directory environment.
Contributor Issues Stars Forks
GitHub - optiv/Talon:...
A password guessing t...
github.com

Apr 29, 2021

 n00py Retweeted 

 **Nick Carr**
@ItsReallyNick



Replying to @ItsReallyNick



 REMINDER:

This is a fast-paced field.
You can't always be first, but
you can often be the first to
be right. Or the first to be
thorough.

This applies to leading a
#DFIR investigation, writing
#threatintel, and security
journalism.



Work with people that
challenge hypotheses.



  Nov 17, 2018

 **n00py**
@n00py1 


Replying to @n00py1


Another one I remembered,
Outlook Web Access (OWA)
might prompt for it


  Sep 16, 2021

 **n00py**
@n00py1 


Thanks to everyone so far for
commenting other methods.
Going to test them all when I
can and post a
comprehensive blog
<https://twitter.com/n00py1/status/1438528686332973065>


  Sep 16, 2021



 n00py Retweeted 

 **mpgn**
@mpgn_x64

Thanks to @qtc_de a new
module has arrived on
CrackMapExec to detect if
the WebClient service is
running or not ! 🙌
[github.com/byt3bl33d3r/Cr...](https://github.com/byt3bl33d3r/CrackMapExec/blob/master/modules/webclient.py)
[twitter.com/tifkin_/status...](https://twitter.com/tifkin_/status/1419806476353298442)
[https://twitter.com/tifkin_/stat](https://twitter.com/tifkin_/status/1419806476353298442)
[us/1419806476353298442](https://twitter.com/tifkin_/status/1419806476353298442)



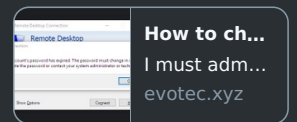
  Sep 16, 2021

 **n00py**
@n00py1 

Replying to @n00py1

Messed up the link,
sorry:[superuser.com/a/13973](https://superuser.com/a/1397397)
[97evotec.xyz/how-to-](https://superuser.com/a/1397397)
[change-...](https://superuser.com/a/1397397)

If anyone else has other ways
to do this (anonymous/non-
admin) let me know! Always
looking to learn more
techniques. (3/3)



Sep 16, 2021



n00py

@n00py1



Replying to @n00py1

If you find one, you can RDP anonymously and then change the password in the GUI.

Also, if you have any user session (non admin) via

CATEGORIES

Select Category



Copyright © 2021, n00py Blog.

[Home](#)

[Defense](#)

[Github](#)

[LinkedIn](#)

[OSX](#)

[Pentesting](#)

[Research](#)

[Walkthroughs](#)

[whoami](#)