Hacking Viral

All About Ethical Hacking Tutorials for beginner or intermediate with simple step by step, also covering how to hack Facebook, wifi, computer etc.

=[Home]= =[General]= =[Metasploit]= =[Programing]= =[Networking]= =[Windows]= =[Linux]= =[Malware]= =[Contact]=

Tutorials

Android
Android-Tools
Anonymous web surfing
Applications
Backdoors
Bash-Script
Bitcoin
botnets
Broadband
Browser Security
Bruteforce-Attack
BSD
bug bounty
Bypass
Capture The Flag
certifications
Challenge
Cloning
Computer Forensics
Computer hacking
contests
Course Reviews
Cryptography
cyberwar
DDOS Attack
Debian
Documentary
DOM XSS
Ebooks
email
espionage
Forensics-Tool
FreeBSD
Freewares
Gadgets
General
Guides
Hack Facebook
Hack-Tools
Hacked
Hacker The Dude News
hackers
Hacking
Hacking basics
Hacking News
Hacking Windows
HackingTools
How-To-Guides
Inspire-Yourself
Interviews
iOS
iOS-Tools
iPhone
Joomla Security
Kali-Linux

DotDotPwn - Directory Traversal Fuzzer

Date : April 30, 2017
Category : Hacking - HackingTools - Pearl - SecurityTools - Vulnerability - Vulnerability_Scanners
Author : AC10 Writer
Responds : 0 Comment

Share Google Facebook Twitter More

DotDotPwn - Directory Traversal Fuzzer - Hello Hackers Hacking Viral, In the article you read this time with the title DotDotPwn - Directory Traversal Fuzzer, we have prepared This article is good for you to read and take information in it. Hopefully post content Article Hacking, Article HackingTools, Article Pearl, Article SecurityTools, Article Vulnerability, Article Vulnerability_Scanners, that we write you can understand it.

Read another post

- Logon Warning Hack Windows
- Hack Your Friend To Get His Browser Info And Ip address
- Script Check Network Connectivity With Power of PowerShell
- XSSF - Cross-Site Scripting Framework
- Pentoo - Gentoo-Based Linux Distribution For Penetration Testers
- Weevely - Weaponized Web Shell
- DotDotPwn - Directory Traversal Fuzzer
- Hackode - Android App For Hackers
- Web-Sorrow - Tool For Detecting Misconfigurations and Collecting Server Information
- Hashcat - An Advanced Password Cracking Tool
- ASLR Process Scanner - Tool For Identifying ASLR Enabled Processes
- WhatWeb - An Advanced Website Fingerprinter
- Advanced Windows Service Manager - Tool For Analyzing Windows Services
- SSLyze - Tool For Analysing SSL/TLS Configurations
- Acunetix - Web Vulnerability Scanner For Hackers
- Qualys BrowserCheck - An Online Security Scanner
- Xenotix - XSS Vulnerability Detection and Exploitation Framework
- Netsparker - Web Application Vulnerability Scanner For Hackers
- Around The Hacks In 90 seconds #1
- Basic Batch File Programming free

DotDotPwn - Directory Traversal Fuzzer

Search For

Enter keywords here...

Popular Post

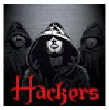
Hashcat - An Advanced Password Cracking Tool
Hashcat is an advanced password cracking program that supports five unique modes of attack: Straight , Combination , Brute-force , Hybrid di...

How to make a fake virus in windows
Ok this one is great and the great thing is its Video Supported !! I owe you this video tutorial , because there are many ...

How To Make Dark Angel's Phunky Virus

```
   //==//  //  //  /||
  //      //====
  //==//  //|  //    //  //
  //  //  //||     //     //
//  //  //||  //   //==//  //==...
```

Xortool - A Tool To Analyze Multi-byte XOR Cipher
Xortool is a python tool that allows you to analyze multi-byte xor cipher and guess the xor key (based on count of equal chars) and the key ...

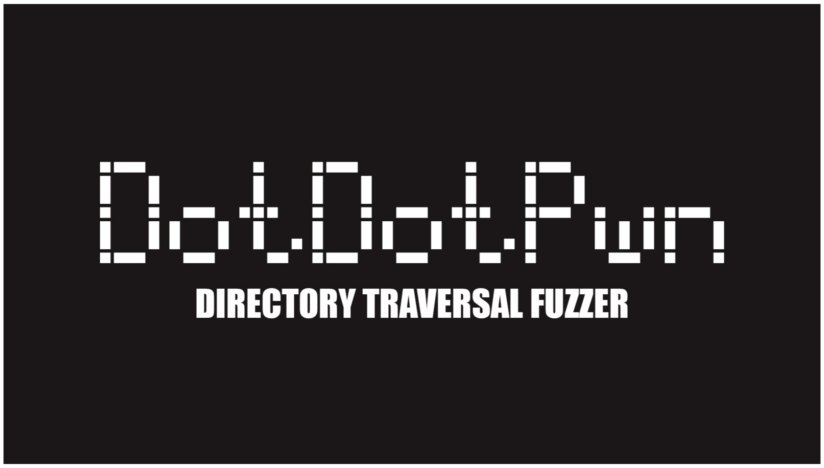


How to begining in the World of Hacking?
When I got into hacking, i realized that there wasnt many text philes for newbies. so, i decided to write one. i dont really care about...

Hackode - Android App For Hackers
Updated on 28-April-2017 Hackode is an android app developed by Ravi Kumar for penetration testers, ethical hackers, IT admi...

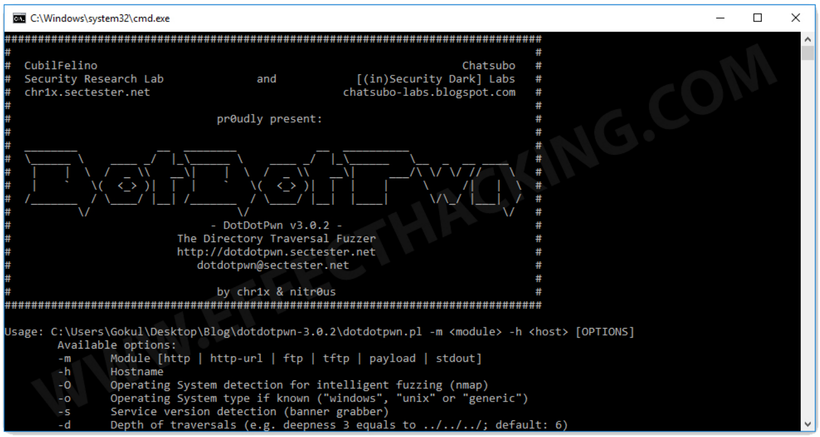
Script Check Network Connectivity With Power of PowerShell

Linux
Linux-Hacking-Tools
List_Articles
Lock Picking
Mac-Hacking-Tools
Mac-OSX
Malwares
manifesto
Metasploit
NetBSD
Network Security
Networking
Offers
Online-Tools
OpenBSD
Others
OWASP
Parental Control softwares
Password Cracking
Password Hacking softwares
paypal
Pearl
Pentest
Perl
PHP
Presentations
Programing
Python-Script
Ruby
Security tips
Security-Measures
SecurityTools
Small Hacks
Smartphones
Spoofing
spying
sql injection
SQLi-Vulnerability
SSI Vulnerability
SunOS
surveillance
swf vulnerabilities
Talks
TED-Talks
Tools
Tricks
Ubuntu
Videos
Virus's
Vulnerability
Vulnerability_Scanners
waf
Webserver Security
Website hacking
Weekly Top 10 Internet Tools
Whitepapers
Windows
Windows-10
Windows-7
Windows-8
Windows-Hacking-Tool
Windows-Hacks
Windows-XP
Wordpress Security
xss



DotDotPwn is a very flexible intelligent fuzzer that you can use to discover traversal directory vulnerabilities in Web/FTP/TFTP servers and Web platforms (CMSs, ERPs, Blogs, etc). It is written in Perl programming language and can be run either under OS X, *NIX or Windows platforms.

Also, it has a protocol-independent module to send the desired payload to the host and port specified. On the other hand, it also could be used in a scripting way using the STDOUT module.



```
################################################################################
#                                                                              #
#  CubilFelino                                                       Chatsubo  #
#  Security Research Lab              and             [(in)Security Dark] Labs #
#  chr1x.sectester.net                               chatsubo-labs.blogspot.com #
#                                                                              #
#                               pr0udly present:                               #
#                                                                              #
#                                                                              #
#                              - DotDotPwn v3.0.2 -                            #
#                         The Directory Traversal Fuzzer                       #
#                         http://dotdotpwn.sectester.net                       #
#                            dotdotpwn@sectester.net                           #
#                                                                              #
#                               by chr1x & nitr0us                             #
################################################################################

Usage: C:\Users\Gokul\Desktop\Blog\dotdotpwn-3.0.2\dotdotpwn.pl -m <module> -h <host> [OPTIONS]
        Available options:
        -m      Module [http | http-url | ftp | tftp | payload | stdout]
        -h      Hostname
        -O      Operating System detection for intelligent fuzzing (nmap)
        -o      Operating System type if known ("windows", "unix" or "generic")
        -s      Service version detection (banner grabber)
        -d      Depth of traversals (e.g. deepness 3 equals to ../../../; default: 6)
```

Fuzzing modules supported in this version:

- HTTP
- HTTP URL
- FTP
- TFTP
- Payload (Protocol independent)
- STDOUT

What are the requirements?

- Perl (Programmed and tested on Perl 5.8.8 and 5.10).
- Nmap (Only if you plan to use the OS detection feature. This requires root privileges).

```
Usage: dotdotpwn.pl -m <module> -h <host> [OPTIONS]

Available options:

-m      Module [http | http-url | ftp | tftp | payload | stdout]

-h      Hostname

-O      Operating System detection for intelligent fuzzing (nmap)

-o      Operating System type if known ("windows", "unix" or "generic")

-s      Service version detection (banner grabber)

-d      Depth of traversals (e.g. deepness 3 equals to ../../../; default: 6)

-f      Specific filename (e.g. /etc/motd; default: according to OS detected,

        defaults in TraversalEngine.pm)

-E      Add @Extra_files in TraversalEngine.pm
```

Some days ago i got some scripts from one of my friend which was certain to use when pentesting stuff for Testing the internet connectivity...

Knockpy - A Subdomain Scanner
Knockpy is a Python script written by security researcher Gianni 'guelfoweb' Amato , that can enumerate subdomains on a target domai...

User's Guide to Hacking | Newbie's
User's guide Well, howdi folks... I guess you are all wondering who's this guy (me) that's trying to show you a bit of every...

PwnPi - A Pen-testing Drop Box Distribution For Raspberry Pi
PwnPi is a Linux-based penetration testing drop box distribution for the Raspberry Pi . It currently has 200+ security tools pre-installed t...

Blog Archive

▼ 2017 (110)
► June (7)
► May (33)
▼ April (26)
DotDotPwn - Directory Traversal Fuzzer
Hackers Wanted (Documentary Film)
Hackode - Android App For Hackers
Xortool - A Tool To Analyze Multi-byte XOR Cipher
ARPwner - ARP & DNS Poisoning Attack Tool
14 Best Songs (Poems) About Hacking
ADHD - An Ubuntu Based

Translate

Select Language ▼
Powered by Google Translate

Powered by Blogger.

```
        (e.g. web.config, httpd.conf, etc.)
-S      Use SSL for HTTP and Payload module
        (not needed for http-url, use a https:// url instead)
-u      URL with the part to be fuzzed marked as TRAVERSAL
        (e.g. http://foo:8080/id.php?x=TRAVERSAL&y=31337)
-k      Text pattern to match in the response
        (http-url & payload modules - e.g. "root:" if trying /etc/passwd)
-p      Filename with the payload to be sent and the part
        to be fuzzed marked with the TRAVERSAL keyword
-x      Port to connect (default: HTTP=80; FTP=21; TFTP=69)
-t      Time in milliseconds between each test
        (default: 300 (.3 second))
-X      Use the Bisection Algorithm to detect the exact
        deepness once a vulnerability has been found
-e      File extension appended at the end of each fuzz string
        (e.g. ".php", ".jpg", ".inc")
-U      Username (default: 'anonymous')
-P      Password (default: 'dot@dot.pwn')
-M      HTTP Method to use when using the 'http'
        module [GET | POST | HEAD | COPY | MOVE] (default: GET)
-r      Report filename (default: 'HOST_MM-DD-YYYY_HOUR-MIN.txt')
-b      Break after the first vulnerability is found
-q      Quiet mode (doesn't print each attempt)
-C      Continue if no data was received from host
```

EXAMPLES:

- **HTTP Module**

```
./dotdotpwn.pl -m http -h 192.168.1.1 -x 8080 -f /etc/hosts -k "localhost" -d 8 -t 200 -s
```

The Traversal Engine will create fuzz pattern strings with 8 levels of deepness, then DotDotPwn will send 5 requests per second (-t) against the Web server (-m) listening on port 8080 (-x) and installed in 192.168.1.1 (-h). Additionally, this will try to retrieve the /etc/hosts file (-f) and to avoid false positives, an extra check will be done against the server's response in order to find the "localhost" keyword within, if so, it's considered vulnerable. Also, for extra information, the webserver's banner will be retrieved (-s). DotDotPwn will save the scan results in a filename called 192.168.1.1_<date>_<hour> in the Reports folder.

```
./dotdotpwn.pl -m http -h 192.168.1.1 -O -X -M POST -e .php -E
```

DotDotPwn will try to detect the Operating System running on the target (-O) and once detected, the Traversal Engine will create fuzz patterns according to the OS detected. After that, all the HTTP requests will be adapted to the method specified, in this case, the POST method instead GET (-M). At the end of each fuzz request, the extension .php will be appended (-e). The -E flag tells DotDotPwn to look for the @Extra_files defined in TraversalEngine.pm (by default, "config.inc.php" and "web.config"). Finally, we have enabled the Bisection Algorithm (-X) to detect the exact deepness of a vulnerability, so if a vulnerability is found, this algorithm will try to detect the exact deepness with the minimum number of requests.

- **HTTP URL Module**

```
./dotdotpwn.pl -m http-url -u http://192.168.1.1:10000/unauthenticated/TRAVERSAL -O -k "root:" -r webmin.txt
```

DotDotPwn will try to detect the Operating System running on 192.168.1.1 (-O) and once detected, the Traversal Engine will create the fuzz patterns according to the OS detected. After that, the Engine will replace the TRAVERSAL token within the specified URL (-u) by the traversal patterns created and will send the fuzzed request against the Web server listening on port 10000. Finally, to avoid false positives, an extra check will be done against the server's response in order to find the "root:" keyword within, if so, it's considered vulnerable. Supposing that the file to retrieve is /etc/passwd, is almos *sure* that the "root:" keyword is at the beginning of the file. DotDotPwn will save the scan results in a filename called webmin.txt in the Reports folder.

- **FTP Module**

```
./dotdotpwn.pl -m ftp -h 192.168.1.1 -s -U nitr0us -P n1tr0u5pwnzj00 -o windows
-q -r ftp_server.txt
```

First off all, DotDotPwn will try to obtain the banner message (-s) of the FTP Server (-m), and then, will try to log in with the specified username (-U) and password (-P) in case of the server doesn't allow anonymous access. Once authenticated, it will try to get well-known files in windows operating systems (-o) in the "retrieved_files" local folder. Also, DotDotPwn won't print the details of each attempt, instead, it will work in quiet mode (-q) and will only print the vulnerable traversal patterns detected. It will then save the scan results in a filename called ftp_server.txt (-r) in the Reports folder.

- **TFTP Module**

```
./dotdotpwn.pl -m tftp -h 192.168.1.1 -b -t 1 -f
windows/system32/drivers/etc/hosts
```

DotDotPwn will send a traversal pattern against the TFTP server (-m) serving in 192.168.1.1 (-h) each 1 millisecond, that means, as fast as possible. And then, DotDotPwn will finish the fuzz testing when it has found the first vulnerability (-b). The fuzz testing will be targeting the specific file located in windows/system32/drivers/etc/hosts (-f). DotDotPwn will save the scan results in a filename called 192.168.1.1_<date>_<hour> in the Reports folder.

- **PAYLOAD Module**

```
./dotdotpwn.pl -m payload -h 192.168.1.1 -x 10000 -p payload_sample_1.txt -k
"root:" -f /etc/passwd
```

The Traversal Engine will replace the TRAVERSAL token within the specified payload file (-p) by the traversal patterns created and will send the fuzzed payload against the tcp server (in this example we're supposing that is Webmin) listening on port 10000 (-x) and installed in 192.168.1.1 (-h). Finally, DotDotPwn will look for the "root:" keyword (-k) in the server's response, and if it appears, it's considered vulnerable. Supposing that the file to retrieve is /etc/passwd (-f), is almost *sure* that the "root:" keyword is at the beginning of the file. DotDotPwn will save the scan results in a filename called 192.168.1.1_<date>_<hour> in the Reports folder.

- **STDOUT Module**

```
./dotdotpwn.pl -m stdout -d 5
```

The Traversal Engine will create fuzz pattern strings with 8 levels of deepness and DotDotPwn will print the results to STDOUT, so you can use it as you wish, by example, passing the traversal patterns as a parameter to another application, pipe, socket, etc.

Happy fuzzing!

Download DotDotPwn (GitHub)

Download DotDotPwn 3.0.2.zip

Download DotDotPwn 3.0.2.tar.gz

Such is the article DotDotPwn - Directory Traversal Fuzzer

This is the article DotDotPwn - Directory Traversal Fuzzer this time, hopefully can benefit for you all. Well, see you in other article post.

You are now reading the **DotDotPwn - Directory Traversal Fuzzer**

0 Comments Sort by Newest

Add a comment...

Facebook Comments plug-in

by

Facebook Comment

Related Tutorials :

Hacking

- Around The Hacks In 90 seconds #1
- Basic Batch File Programming free
- Logon Warning Hack Windows
- Hack Your Friend To Get His Browser Info And Ip address
- Script Check Network Connectivity With Power of PowerShell
- How to Hack Someones ISP Password
- Windows 7 GodMode Hack

Post a Comment

Enter your comment...

Comment as: Select profile... ▼

Publish Preview

← Next Post Home Prev Post →