

Forum:[Hack Forums](#)

Thread: [\[FREE\] XML-RPC SCANNER || FREE || THREADS || FAST || 100% WORKS](#)

Zinedine Zidane - August 28, 2014, 9:26 am

Hey Everyone it's Zidane, today i coded a New XML-RPC Scanner, more faster, easy to scan

You can scan the whole world in 6H if you have a 100mbps private connection.

Requierments

- A Server with a good connection
- Perl installed
- a Brain

Modules

1st you need to install all modules to use the script

- HTML::Parser

```
Code wget http://search.cpan.org/CPAN/authors/id/G/GA/GAAS/HTML-Parser-3.71.tar.gz
tar -xvf HTML-Parser-3.71.tar.gz
cd HTML-Parser-3.71
perl Makefile.PL
make
make install
- LWP::UserAgent
```

```
Code wget http://search.cpan.org/CPAN/authors/id/M/MS/MSCHILLI/libwww-perl-6.08.tar.gz
tar -xvf libwww-perl-6.08.tar.gz
cd libwww-perl-6.08
perl Makefile.PL
make
make install
- LWP::Simple
```

```
Code wget http://search.cpan.org/CPAN/authors/id/M/MS/MSCHILLI/libwww-perl-6.08.tar.gz
tar -xvf libwww-perl-6.08.tar.gz
cd libwww-perl-6.08
perl Makefile.PL
make
make install
- Parallel::ForkManager
```

```
Code wget
http://search.cpan.org/CPAN/authors/id/S/SZ/SZABGAB/Parallel-ForkManager-1.06.tar.gz
tar -xvf Parallel-ForkManager-1.06.tar.gz
cd Parallel-ForkManager-1.06
perl Makefile.PL
```

```
make
make install
- Net::IP
```

```
Code wget http://search.cpan.org/CPAN/authors/id/M/MA/MANU/Net-IP-1.26.tar.gz
tar -xvf Net-IP-1.26.tar.gz
cd Net-IP-1.26
perl Makefile.PL
make
make install
Set up the script
```

Source code

```
Code #! /usr/bin/perl
```

```
use HTML::Parser; #HTML
use LWP::UserAgent; #http request
use LWP::Simple;
use Parallel::ForkManager; # threads
use strict;
use Net::IP; # range IP
use IO::Socket;
use Term::ANSIColor;
use vars qw( $PROG );
( $PROG = $0 ) =~ s/^\.[V\\]//;
#Usage
if ( @ARGV == 0 ) {
    print "Usage : ./$PROG [Start IP] [End IP] [Threads] [.txt] [Delay]\n Coded by Zidane For HF
User\n";
    exit;
}
my $threads = $ARGV[2]; #threads
my @ip_team = (); #IP
$|= 1;
my $ip = new Net::IP ("$ARGV[0] - $ARGV[1]") or die "Invalid IP Range.". Net::IP::Error() ."\n";
$SIG{'INT'} = sub {exit;};
my @folders = ("/wordpress/", "/wp/", "/blog/", "/"); # folders
my $stringsearch = "XML-RPC"; # string to search
my $filename = $ARGV[3]; # .txt
my $max_processes = $ARGV[2]; #threads
my $pm = Parallel::ForkManager->new($max_processes); # thread spawner

#Forking
while ($ip) {
    push @ip_team, $ip++ ->ip();
    if ( $threads == @ip_team ) { Scan(@ip_team); @ip_team = () }
}
Scan(@ip_team);

#Scan
sub Scan
{
```

```
my @Pids;
```

```
foreach my $ip (@_)
{
    my $pid    = fork();
    die "Can't Fork $!\n" unless defined $pid;
```

```
    if (0 == $pid)
    {
        alarm 1;
```

```
foreach (@folders) {
```

```
    my $pid2 = $pm->start and next; #thread
    alarm("$ARGV[4]");
```

```
    my $url = "http://$ip" . "$_" . "xmlrpc.php";
    my $ua = LWP::UserAgent->new;
    print "\e[96m[!]Search \e[31m$url\n\e[0m";
    my $response = $ua->get($url);
    if ( !$response->is_success ) {
    }
    if (head($url)) {
```

```
        my $parser = HTML::Parser->new( 'text_h' => [ \&text_handler, 'dtext' ] ); #text decoder
        $parser->parse( $response->decoded_content );
        sub text_handler {
            chomp( my $text = shift );
```

```
            if ( $text =~ /$stringsearch/i ) {
```

```
                my $ui = $url;
                $ui =~ s/xmlrpc.php/?feed=rss2/;
                if (head($ui)) {
                    sub check {
                        $LOLGETIT=get($ui);
                        $LOLGETIT =~ /<item>.+?<link>(.*?)</link>.+?</item>/s;
                        if ($1) {
                            open (FILE, ">>$filename");
                            my $post = $1;
                            $ui =~ s/{Q?feed=rss2\E}{xmlrpc.php};
                            print FILE "$ui $post\n";
                        }
                    }
                    close (FILE);
                    print "\e[96m[+]Found : \e[32m$ui $post\e[0m\n";
                    exec($^X, "-e", "sleep 1,kill(0,$pid2)||kill -9,$pid2"); #kill process
                }
            }
            check();
        } else {
        }
    }
} else {
}
```

```
$pm->finish;  
}
```

```
    exit  
    }  
    else  
    {  
    push @Pids, $pid  
    }  
    }
```

```
foreach my $pid (@Pids) { waitpid($pid, 0) }  
}
```

Usage perl scan.pl [Start IP] [End IP] [Threads] [.txt] [Delay]

Thanks to Vyp0r i recode his basic Scanner (<http://pastebin.com/xYPux8dF>)

Please do not forget to say "Thanks" if i helped you

Infected. - December 28, 2014, 7:01 am

Global symbol "\$LOLGETIT" requires explicit package name at perl.pl line 74.

Zinedine Zidane - December 28, 2014, 7:34 am

(Dec 28, 2014 08:01 AM)Infected. Wrote: [\[CITE\]](#) Global symbol "\$LOLGETIT" requires explicit package name at perl.pl line 74.

delete the "use:strict;" at the begining

Infected. - December 28, 2014, 7:40 am

Please private message me your skype.

Zinedine Zidane - December 28, 2014, 7:59 am

(Dec 28, 2014 08:40 AM)Infected. Wrote: [\[CITE\]](#) Please private message me your skype.

Allright Speak on skype then

Regards

?

Infected. - December 28, 2014, 8:21 am

He helped me fix the problem vouch for this guy:)

Zinedine Zidane - January 1, 2015, 12:35 pm

(Dec 28, 2014 09:21 AM)Infected. Wrote: [\[CITE\]](#) He helped me fix the problem vouch for this guy:)

No problem, It's normal to help you !

Regards

?

Tatishchev - January 1, 2015, 12:46 pm

Thanks for sharing.... I appreciate it. :)

Zinedine Zidane - January 4, 2015, 4:20 pm

(Jan 1, 2015 01:46 PM)Tatishchev Wrote: [\[CITE\]](#) Thanks for sharing.... I appreciate it. :)
You welcome I hope you like it

Regards

meskone - January 10, 2015, 6:53 pm

One of the best users on HF !! HQ !! Voucher for you and of the for your tools ;)

meskone - January 13, 2015, 9:12 am

```
[root@host dos]# perl scan.pl 1.0.0.0 255.255.255.255 8 scann.txt
Can't locate Encode/Locale.pm in @INC (@INC contains: /usr/local/lib64/perl5
/usr/local/share/perl5 /usr/lib64/perl5/vendor_perl /usr/share/perl5/vendor_perl /usr/lib64/perl5
/usr/share/perl5 .) at /usr/local/share/perl5/LWP/UserAgent.pm line 1001.
Compilation failed in require at scan.pl line 5.
BEGIN failed--compilation aborted at scan.pl line 5.
```

Zinedine Zidane - January 13, 2015, 9:20 am

```
(Jan 13, 2015 10:12 AM)meskone Wrote: \[CITE\] [root@host dos]# perl scan.pl 1.0.0.0
255.255.255.255 8 scann.txt
Can't locate Encode/Locale.pm in @INC (@INC contains: /usr/local/lib64/perl5
/usr/local/share/perl5 /usr/lib64/perl5/vendor_perl /usr/share/perl5/vendor_perl /usr/lib64/perl5
/usr/share/perl5 .) at /usr/local/share/perl5/LWP/UserAgent.pm line 1001.
Compilation failed in require at scan.pl line 5.
BEGIN failed--compilation aborted at scan.pl line 5.
Install Encode::locale
```

Regards ?

regexks_ - January 13, 2015, 9:20 am

```
(Jan 13, 2015 10:12 AM)meskone Wrote: \[CITE\] [root@host dos]# perl scan.pl 1.0.0.0
255.255.255.255 8 scann.txt
Can't locate Encode/Locale.pm in @INC (@INC contains: /usr/local/lib64/perl5
/usr/local/share/perl5 /usr/lib64/perl5/vendor_perl /usr/share/perl5/vendor_perl /usr/lib64/perl5
/usr/share/perl5 .) at /usr/local/share/perl5/LWP/UserAgent.pm line 1001.
Compilation failed in require at scan.pl line 5.
BEGIN failed--compilation aborted at scan.pl line 5.
You need to install the Encode::Locale Perl module:
```

Code cpan -i Encode::Locale

meskone - January 13, 2015, 12:07 pm

thx you both ;)

HF needs more high skilled ppl like you !

cheers

Socrates???? - January 14, 2015, 12:22 pm

```
(Jan 13, 2015 10:12 AM)meskone Wrote: \[CITE\] [root@host dos]# perl scan.pl 1.0.0.0
255.255.255.255 8 scann.txt
Im not sure if you should do that. This script seems to take a long time to scan. I suggest trying
specific ip ranges, ect
```

Zinedine Zidane - January 14, 2015, 12:25 pm

(Jan 14, 2015 01:22 PM)Socrates™ Wrote: [\[CITE\]](#) Im not sure if you should do that. This script seems to take a long time to scan. I suggest trying specific ip ranges, ect
Perl loops are Very slow

Regards

Socrates???? - January 14, 2015, 12:31 pm

(Jan 14, 2015 01:25 PM)Zinedine Zidane Wrote: [\[CITE\]](#) Perl loops are Very slow

Regards

Yes i have noticed as i experimented with the scanner. Im not really sure but it looked as if it was only going through at about 25 ip/s. Which i mean that would take ages to scan. There are also a few problems in the source:

Code my @folders = ("/wordpress/", "/wp/", "blog", "/");When scanning the output of this is sometimes 1.1.1.1blog

Pretty sure around the blog there should be 2 / .

so it would look like this:

Code my @folders = ("/wordpress/", "/wp/", "/blog/", "/");

Here is the code you provided:

My edit to your code:

Zinedine Zidane - January 14, 2015, 1:34 pm

(Jan 14, 2015 01:31 PM)Socrates™ Wrote: [\[CITE\]](#) Yes i have noticed as i experimented with the scanner. Im not really sure but it looked as if it was only going through at about 25 ip/s. Which i mean that would take ages to scan. There are also a few problems in the source:

Code my @folders = ("/wordpress/", "/wp/", "blog", "/");When scanning the output of this is sometimes 1.1.1.1blog

Pretty sure around the blog there should be 2 / .

so it would look like this:

Code my @folders = ("/wordpress/", "/wp/", "/blog/", "/");

Here is the code you provided:

My edit to your code:

Yeah I Saw

I'm actually working on a C version able to scan the whole world un 5-10h with a pur 1gbps uplink dedi

regexks_ - January 14, 2015, 4:05 pm

(Jan 14, 2015 02:34 PM)Zinedine Zidane Wrote: [\[CITE\]](#) Yeah I Saw

I'm actually working on a C version able to scan the whole world un 5-10h with a pur 1gbps uplink dedi

This has existed for a very long time, although the old C version was removed in light of the much better Go version: [zgrab](#).

Zinedine Zidane - January 14, 2015, 9:56 pm

(Jan 14, 2015 05:05 PM)regexks_ Wrote: [\[CITE\]](#) This has existed for a very long time, although the old C version was removed in light of the much better Go version: [zgrab](#).

Nice

Yes I know that there is a Pingback Scanner but I want code one to train

drt420 - February 4, 2015, 1:21 am

getting below errors pls help?

Code [!]
Search http://1.0.5.170blogxmlrpc.php
Cannot fork: Cannot allocate memory at /usr/local/share/perl/5.14.2/Parallel/ForkManager.pm line 515.
[!]
Search http://1.0.5.168/xmlrpc.php
[!]
Search http://1.0.5.172/wp/xmlrpc.php
[!]
Search http://1.0.5.170/xmlrpc.php
Cannot fork: Cannot allocate memory at /usr/local/share/perl/5.14.2/Parallel/ForkManager.pm line 515.
[!]
Search http://1.0.5.169/xmlrpc.php
[!]
Search http://1.0.5.171blogxmlrpc.php
[!]
Search http://1.0.5.172/wordpress/xmlrpc.php
Cannot fork: Cannot allocate memory at /usr/local/share/perl/5.14.2/Parallel/ForkManager.pm line 515.
[!]
Search http://1.0.5.171/xmlrpc.php
[!]
Search http://1.0.5.171/wp/xmlrpc.php
Cannot fork: Cannot allocate memory at /usr/local/share/perl/5.14.2/Parallel/ForkManager.pm line 515.
Can't Fork Cannot allocate memory

Zinedine Zidane - February 4, 2015, 1:31 am

(Feb 4, 2015 02:21 AM)drt420 Wrote: [\[CITE\]](#) getting below errors pls help?

Code [!]
Search http://1.0.5.170blogxmlrpc.php
Cannot fork: Cannot allocate memory at /usr/local/share/perl/5.14.2/Parallel/ForkManager.pm line 515.
[!]
Search http://1.0.5.168/xmlrpc.php
[!]
Search http://1.0.5.172/wp/xmlrpc.php
[!]
Search http://1.0.5.170/xmlrpc.php
Cannot fork: Cannot allocate memory at /usr/local/share/perl/5.14.2/Parallel/ForkManager.pm line 515.
[!]
Search http://1.0.5.169/xmlrpc.php
[!]
Search http://1.0.5.171blogxmlrpc.php
[!]
Search http://1.0.5.172/wordpress/xmlrpc.php
Cannot fork: Cannot allocate memory at /usr/local/share/perl/5.14.2/Parallel/ForkManager.pm line 515.
[!]
Search http://1.0.5.171/xmlrpc.php
[!]
Search http://1.0.5.171/wp/xmlrpc.php
Cannot fork: Cannot allocate memory at /usr/local/share/perl/5.14.2/Parallel/ForkManager.pm line 515.
Can't Fork Cannot allocate memory
How many threads did you use ?

Regards

drt420 - February 4, 2015, 1:32 am

(Feb 4, 2015 02:31 AM)Zinedine Zidane Wrote: [\[CITE\]](#) How many threads did you use ?

Regards

I have 16 core cpu and I have used 8 threads.

Zinedine Zidane - February 4, 2015, 1:33 am

(Feb 4, 2015 02:32 AM)drt420 Wrote: [\[CITE\]](#) I have 16 core cpu and I have used 8 threads.

Weird, Weird

Try with one thread

Regards

drt420 - February 4, 2015, 1:39 am

(Feb 4, 2015 02:33 AM)Zinedine Zidane Wrote: [\[CITE\]](#) Weird, Weird

Try with one thread

Regards

Same issue with 1 thread too :(dont know whats wrong

Zinedine Zidane - February 4, 2015, 1:44 am

(Feb 4, 2015 02:39 AM)drt420 Wrote: [\[CITE\]](#) Same issue with 1 thread too :(dont know whats wrong
try to make a re search on google

Works fine for me and for most other users

6700 - June 1, 2015, 3:08 pm

Code Can't locate HTTP/Request.pm in @INC (you may need to install the HTTP::Request module)
(@INC contains: /etc/perl /usr/local/lib/x86_64-linux-gnu/perl/5.20.2 /usr/local/share/perl/5.20.2
/usr/lib/x86_64-linux-gnu/perl5/5.20 /usr/share/perl5 /usr/lib/x86_64-linux-gnu/perl/5.20
/usr/share/perl/5.20 /usr/local/lib/site_perl .) at /usr/local/share/perl/5.20.2/LWP/UserAgent.pm line
10.

BEGIN failed--compilation aborted at /usr/local/share/perl/5.20.2/LWP/UserAgent.pm line 10.

Compilation failed in require at xml.pl line 4.

BEGIN failed--compilation aborted at xml.pl line 4.

What I'm missing and how can I install it? o.O (Debian 8)

ma?ns - June 10, 2015, 3:06 am

Vouch for this guy, thanks alot

Zinedine Zidane - June 25, 2015, 6:33 am

(Jun 10, 2015 03:06 AM)Foxxi_ Wrote: [\[CITE\]](#) Vouch for this guy, thanks alot
thanks for the comment

Regards

??

Construction - June 25, 2015, 7:37 am

Lol thanks for this script it can help me a bit on scanning RDP's :)

Kotone - October 19, 2015, 9:07 am

Attempt to reload HTTP/Message.pm aborted.

Compilation failed in require at (eval 4) line 2.

...propagated at /usr/share/perl/5.18/base.pm line 83.

BEGIN failed--compilation aborted at /usr/local/share/perl/5.18.2/HTTP/Response.pm line 6.

Compilation failed in require at /usr/local/share/perl/5.18.2/LWP/UserAgent.pm line 11.

BEGIN failed--compilation aborted at /usr/local/share/perl/5.18.2/LWP/UserAgent.pm line 11.

Compilation failed in require at scan.pl line 4.
BEGIN failed--compilation aborted at scan.pl line 4.

3yZtwgIFSCUs - *May 25, 2016, 2:27 am*

sorry for thread bump but this seem look ideally for somewhat layer 7 amplication but what is ip range to scan :)

©Ratatouille™ - *February 8, 2017, 5:39 am*

any guys have xml rpc scanner ?
the script crash all my server

Cylow - *February 8, 2017, 5:42 am*

Wrong threads ifnore this

ZwntanosNekros - *May 20, 2017, 5:10 am*

(Feb 8, 2017 06:39 AM)©Ratatouille™ Wrote: [CITE](#) any guys have xml rpc scanner ?
the script crash all my server
Same problem as you , any scanner around that don't crash ??

skyra1453 - *January 4, 2018, 1:33 pm*

Do you have a video narration about its use? I could not

Zinedine Zidane - *March 5, 2021, 12:22 pm*

the tool is still working guys :)