

[TOOL] Multimap – Multithreaded Wrapper for NMap

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-08/0069.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/24/03

To: list@securiteam.com

Date: 24 Aug 2003 16:55:00 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Multimap – Multithreaded Wrapper for NMap

DETAILS

Multimap is a multithreaded wrapper for NMap designed to run a number of concurrent NMap scans and speed up the scan of large networks. Optionally it will launch AMap on the open ports and generate an HTML file of the results.

Tool source:

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

```
#
```

```
# Runs a number of concurrent nmap processes and stores the results in
```

```
# a specified directory in xml, human and machine formats. Optionally runs
```

```
# amap using the nmap output as input. Writes the results to an HTML file
```

```
# in the results directory.
```

```
# Make sure you have the latest nmap and amap (www.thc.org) and that they play
```

```
# nicely together. Tested with nmap 3.27 and amap 4.2.
```

```
#
```

```
# NOTE: Change the values below to match your environment and requirements!
```

```
#
```

Securiteam: [TOOL] Multimap – Multithreaded Wrapper for NMap

```
# by
# Stephen de Vries – stephen at twisteddelight dot org
# www.twisteddelight.org/security
#
#####
use strict;

my $NMAP_COMMAND="/usr/local/bin/nmap";
my $NMAP_OPTIONS="--max_rtt_timeout 2000"; # -oX -oN -oM are set
automatically

my $AMAP_COMMAND="/usr/local/bin/amap";
my $AMAP_OPTIONS="-b -1"; # -o -m are set automatically

my $BAN_WIDTH=50;

#####

my @hosts, my $wdir, my $hostFile, my $procs, my $run_amap;
my @pids; # Store the currently running pids
my %activehosts; # hosts currently being scanned, indexed according to pid
my %banners; # store banner info from amap
my @HTML; # temporary storage for the output

use POSIX qw(:signal_h :errno_h :sys_wait_h);
use Getopt::Std;

$SIG{CHLD} = \&REAPER;
sub REAPER {
    my $pid;
    $pid = waitpid(-1, &WNOHANG);

    if ($pid == -1) {
        # no child waiting. Ignore it.
    } elsif (WIFEXITED($?)) {
my $found=0;
my $i=0;
# Check to see if the pid that exited belongs to one of the nmaps
while ((!$found) && ($i <= $#pids)) {
    if ($pid == $pids[$i]) {
        splice(@pids,$i,1);
        $found=1;
        wlog(0,"Nmap completed on: $activehosts{$pid}");
        if ($run_amap) {
            launch_amap($activehosts{$pid});
        }
        delete $activehosts{$pid};
    }
    $i++;
}
    } else {
```

Securiteam: [TOOL] Multimap – Multithreaded Wrapper for NMap

```
    print "False alarm on $pid.\n";
}
$SIG{CHLD} = \&REAPER; # in case of unreliable signals
}

sub getDate {
    my ($sec,$min,$hour,$mday,$mon,$year,$wday,$yday,$isdst) =
localtime(time);
    return "$year-$mon-$mday $hour:$min:$sec";
}

sub wlog {
    my ($code, @msg) = @_ ;
    if ($code ==0) {
        # Print to screen and log file
        print "@msg\n";
        my $date = getDate();
        print LOG "$date|@msg\n";
    } elsif ($code ==1) {
        # Just print to stdout
        print "@msg\n";
    } elsif ($code ==2) {
        # Just print to the log file
        print "@msg\n";
    } else {
        print "Unknown error code: $code\n";
        print "@msg\n";
    }
}

sub launch {
    my ($host) = @_ ;
    my $OUTPUT="-oX $wdir/xml/$host.nmap.xml -oN
$wdir/human/$host.nmap.human -oM $wdir/machine/$host.nmap.machine";
    my $RUNSTR="$NMAP_COMMAND $NMAP_OPTIONS $OUTPUT $host";
    wlog(0, "Launching: $RUNSTR");
    exec($RUNSTR);
}

sub launch_omap {
    my ($host) = @_ ;
    my $OUTPUT="";
    my $RUNSTR="$AMAP_COMMAND $AMAP_OPTIONS -m -i
$wdir/machine/$host.nmap.machine -o $wdir/omap/$host.omap";
    wlog(0, "Launching: $RUNSTR");
    if (!fork()) {
        exec($RUNSTR);
    }
}
}
```



```

}

sub getbanners {
  my ($host) = @_ ;
  my $line, my @vals;
  open AMAPFILE, "$wdir/amacp/$host.amap" || wlog(0, "Error: Can't open
file $wdir/amacp/$host.amap for reading");
  while ($line = <AMAPFILE>) {
    if ($line =~ /^$host:([0-9]+)([a-z0-9A-Z\-\_]*:){5}(.*)/) {
      my $port = $1; my $ban = $3;
      $ban =~ s:/$/No banner found/;
      $banners{$port} = $ban;
      print ">> $port = $ban\n";
    }
  }
  close AMAPFILE;
}

sub convertToHTML {
  my $dirname = "$wdir/machine/";
  my $line, my $file;
  my $ip, my $hostname, my $os, my $seq, my @ports, my $port, my $stepseq,
my $portslist;
  opendir(DIR, $dirname) or die "can't open dir $dirname: $!";
  open OUTFILE, ">$wdir/machine/allresults.machine.nmap" || die "Can't
open output file: $wdir/machine/allresults.machine.nmap";
  while (defined($file = readdir(DIR))) {
    if (($file =~ /\. /) || ($file =~ /allresults/)) {next;}
    open INFILE, "$wdir/machine/$file" || wlog(0,"Error: Can't open
results file: $wdir/machine/$file\n");
    my @lines = <INFILE>;
    close INFILE;
    print OUTFILE @lines;
  }
  close OUTFILE;
  closedir(DIR);

  ##### Put a header on the html file
  push @HTML, "<HTML><HEAD></HEAD><BODY>\n<H3>Nmap results</H3>\n";

  ##### Process the file
  open FILE, "$wdir/machine/allresults.machine.nmap" || die "Error opening
$wdir/machine/allresults.nmap";
  my @lines = <FILE>;
  close FILE;
  foreach $line (@lines) {
    if ($line =~
/^Host:[s+([0-9\.]*)\s+((\S*))\s+Ports:[s+(*)]\s+(?=[I]gnored)Ignored\
State:(.*)/) {
      my ($ip, $hostname, $portslist,$rest) = ($1,$2,$3,$4);
      getbanners($ip);

```

Securiteam: [TOOL] Multimap – Multithreaded Wrapper for NMap

```

my ($os, $seq) = ("Unknown", "Unknown");
push @HTML, "\n<table width=\"80%\" border=1><tr>\n";
push @HTML, " <td width=120><b>IP
Address</b></td><td>$ip</td></tr>\n";
if (length($hostname > 1)) {
    push @HTML, "
<tr><td><b>Hostname</b></td><td>$hostname</td></tr>\n";
}
if ($rest =~ /\.(.*)((?=OS)OS\:(.*)((?=IPID)IPID\s+Seq\:(.*/)) {
    ($rest,$os, $seq) = ($1,$2,$3);
    push @HTML, " <tr><td><b>OS Guess</b></td><td>$os</td></tr>\n";
    #push @HTML, " <tr><td><b>TCP
Sequence</b></td><td>$tcpseq</td></tr>\n";
    push @HTML, " <tr><td><b>IPID
Sequence</b></td><td>$seq</td></tr>\n";
}
push @HTML, " <tr><td valign=top><b>Ports</b></td><td><table
width=\"100%\" border=1>\n";
push @HTML, "
<tr><td><b>Num</b></td><td><b>Status</b></td><td><b>Proto</b></td><td><b>Name</b></td>";
if ($run_ama) {
    push @HTML, " <td><b>Banner</b></td>";
}
push @HTML, "</tr>\n";
my @ports = split(/,/,$portslist);
foreach $port (@ports) {
    $port =~ s/^\s+//;
    my @list = split(///,$port);
    push @HTML, " <tr><td valign=top>$list[0]</td>\n";
    push @HTML, " <td valign=top>$list[1]</td>\n";
    push @HTML, " <td valign=top>$list[2]</td>\n";
    push @HTML, " <td valign=top>$list[4]</td>\n";
    if ($run_ama) {
        my $banner = $banners{$list[0]};
        $banner =~ s/^\</g;
        $banner =~ s/^\>/g;
        $banner =~ s/\n/\n<br>/g;
        push @HTML, " <td valign=top>$banner</td>";
    }
    push @HTML, "</tr>\n";
}
push @HTML, " </table></td></tr></table>\n<br><br>";
}
}
#### Put a footer on the HTML
push @HTML, "</BODY></HTML>\n";
open OUT, ">$wdir/multimap.html";
print OUT @HTML;
close OUT;
}

```

Securiteam: [TOOL] Multimap – Multithreaded Wrapper for NMap

```
sub usage {
    print STDERR << "EOF";
```

Usage: \$0 -f file -d dir -p processes [-n "options"] [-a] [-h]

-f file : text file containing IP addresses to scan
-d dir : directory to store output files
-p processes : the number of concurrent nmap scans to run

-n "options" : additional nmap options
-a : run amap
-h : this help

Notes:

Change the values of \$NMAP_OPTIONS and \$AMAP_OPTIONS in the code to save from typing your favourite options on the cmd line.

```
EOF
}
```

```
#####
# Start main program
```

```
my %options;
getopts("f:d:p:n:ah", \%options);
$hostFile = $options{"f"};
$wdir = $options{"d"};
$procs = $options{"p"};
my $temp = $options{"n"};
$run_amap = $options{"a"};
$temp =~ s/^//g;
$NMAP_OPTIONS = $NMAP_OPTIONS . " " . $temp;

my $error=0;
if (length($hostFile) == 0) {
    print "Error: Must specify a host file with -f file\n";
    $error=1;
}
unless (open(F, $hostFile)) {
    print "Error: can't open file $hostFile for reading\n";
}
close F;
if (length($wdir) == 0) {
    print "Error: Must specify a working directory with -d dir\n";
    $error=1;
}
if (length($procs) == 0){
    print "Error: Must specify the number of processes to run with -p processes\n";
    $error=1;
}
```

Securiteam: [TOOL] Multimap – Multithreaded Wrapper for NMap

```
}
if ($error == 1) {
    usage();
    exit(1);
}

confirmSettings();
init();
my $i=0, my $host, my $currentpid;
while ($#hosts+1 > 0) {
    if ($i < $procs ) {
        $i++;
        $host = pop @hosts;
        $currentpid = fork();
        push @pids, $currentpid;
        if ($currentpid == 0) {
            launch($host);
            exit(0);
        } else {
            $activehosts{$currentpid}=$host;
        }
    }
}
my $total=0;
for (my $n=0;$n <= $#pids;$n++) {
    if ($pids[$n] != 0) {$total++;}
}
$i = $total;
sleep 1;
}
wait;
convertToHTML;
close LOG;
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:stephen@twisteddelight.org>
Stephen de Vries.

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential,

Securiteam: [TOOL] Multimap – Multithreaded Wrapper for NMap

loss of business profits or special damages.