

Re: iptables and port scan

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-02/1210.html>

From: Lutz Donnerhacke (lutz@iks-jena.de)

Date: 02/13/02

From: lutz@iks-jena.de (Lutz Donnerhacke)
Date: Wed, 13 Feb 2002 10:59:43 +0000 (UTC)

* Cedric Blancher wrote:

> *Dans sa prose, Lutz Donnerhacke (lutz@iks-jena.de) nous ecrivait :*
>> *So please, pretty please, describe how to find out which services are*
>> *offered to the internet by a given (random) host.*
>
> *This a deaf discussion. To get this, you have to try, yes, sure, all you*
> *want. But, it is not a normal behaviour (not an illegal one, please*
> *notice) to do this. I do not "prosecute" anybody, I just _drop_.*

Ok, so in order to determine the offered services, I have to do a portscan.
You claim this abnormal, because normal people are not interested in offered services. Ok, that's fine.

And back to the topic: Please use REJECT in such cases. Be kind to abnormal and irritated users. DENY won't help against bad guys, it only generates problems for you and aour legitimate customers and companies you are in contact with.

>> *I'm really sorry, if I did not notice your proposal.*
>
> *You did not provide me a "good" reason to map all services accessible on*
> *a random host.*

I'm interested in informations and serices others can provide for me.
Sometimes they are very useful.

>> *I'd need to know a special service. (I.e. TCP/25 or TCP/1234)*
>
> *But why ? You gave TCP/25 example : just ask your DNS...*
>
> *cbr@elendil:~\$ host -t MX cartel-securite.fr*
> *cartel-securite.fr MX 5 smtp.cartel-info.fr*
>
> *No portscan.*

Do you know, that RFC say: "If no MX record can be found, use A"?

comp.security.firewalls: Re: iptables and port scan

How determine the service offers for 1234? How to determine the DNS offers on TCP/53? Is AXFR abnormal?

>> *How do I find out those information without requiring services not related to my primary goal I do not have a permit for? How do I determine if you offer FTP oder SSH services?*
>
>*You ISP offers you DNS service.*

I'm the ISP. Does this qualify me to behave abnormal?

>*With this service, you can reach my DNS and my SMTP. You can ask for a website, using www on my domain.*

www is a common CNAME prefix but neither required nor necessary.

>*On this website, you'll find links. If I offer CVS to public, it will be mentionned, if I offer FTP, it will be mentionned, and so on.*

Reading and understanding a website containing links suffice to connect? Should I mention scan.pl once again?

>*If I want you to access a restricted area using FTP or SSH, I will personally email you to give you access, login and pass.*

Definitely. But if I connect without them, I do nothing harmful. You can simply reject my connect packet. Nobody has to care about this.

>> *I found an A record for your hostname. Which services can I derivate from this?*
>
>*The only reference for the services I offer to anonymous user is my website.*
>*My website is called www. Was it so difficult to find ?*

Where is it specified, that all allowed services must published in a machine-unreadable language embedded in HTML received via HTTP connects to port 80 on the machine suffixed by "www."?

In order to obtain the information, that <ftp://mixmaster.anonymizer.com/> is normal and legitimate I have to connect to <http://www.mixmaster.anonymizer.com/> first and search for a permit?

Get real! Nobody does this.

OTOH: To access www.mixmaster.anonymizer.com via HTTP I have to search for a permit on <http://www.mixmaster.anonymizer.com:80/> ?

>*Now, just notice. I drop packets, but I do not prosecute anybody and I do not block portscans.*

comp.security.firewalls: Re: iptables and port scan

DENY will harm you, your customers, your friends, and companies you deal with.
I.e. ident is a common backquery.

*>Feel free to scan hosts and find services you like, you just won't be able
>to use them because they are restricted.*

Fine.

- **Next message:** Nameless: "Re: How to Stealth POP3 Port 110 using NIS2000?"
- **Previous message:** Mark Stolz: "Re: Tiny or Zone Alarm?"
- **In reply to:** Cedric Blancher: "Re: iptables and port scan"
- **Next in thread:** Cedric Blancher: "Re: iptables and port scan"
- **Reply:** Cedric Blancher: "Re: iptables and port scan"
- **Messages sorted by:** [date] [thread] [subject] [author] [attachment]