

RE: ICMP (Ping)

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-09/0333.html>

From: Jay Woody (jay_woody_at_tnb.com)

Date: 09/08/03

Date: Mon, 08 Sep 2003 13:18:51 -0500
To: <security-basics@securityfocus.com>

Sounds about right to me. I guess the statement that I was trying to reply to Tim about earlier (I hope I made it clear it wasn't a question) was:

>> *what some people seem to fail to understand, is that it's*
>> *unlikely someone's going to randomly probe for IP's to just*
>> *randomly attack.*

My only point was that in one simple case. The first one that came to my mind. The case of web defacements, I find there to be an overwhelming majority of people that are not trying to hit someone in particular, but rather do exactly that. They just randomly sweep a range (debatable as to how obviously) and find a couple of poor suckers that have the latest IIS exploit not patched yet. They deface the page, tell Alldas to go get a screen capture and call it a night. No thought. No determining a target based upon hatred or zero day exploits. They just randomly scan a range and go from there. We got from there into a debate on how they scan that range first, but I think the original point still holds. Many times people are hacked by chance. You were just the unlucky sucker.

As far as the ping sweep stuff, to be honest, I wouldn't ever have mentioned it if I had the chance to do it over again. :) Obviously, when my friends were in the defacement scene, we/they did things one way and apparently that isn't what they would do now a days. So blocking ICMP doesn't seem to be bad (if I am right and I pray that I am), just doesn't seem to buy you much according to what I am reading. Again, this is entirely the opposite of my experience, but perhaps I am just extremely lucky in that regard. I'll take luck I guess.

JayW

>>> *"Halverson, Chris" <chris.halverson@encana.com> 09/08/03 01:03PM*
>>>

You both make good points, I understand both sides and see what Jay is saying about the timeouts slowing down a would-be cracker. And I do understand what Tim speaks of when he says that the attacker could be

SecurityFocus BASICS: RE: ICMP (Ping)

trying
to locate a specific vulnerability by scanning specific ports or
writing a
script to locate vulnerabilities(example point and case: scanning OS
fingerprints to locate machines that might have the old IRIX lp
printer
login vulnerability). And as said with the right script written could
cut a
ton of time down. But as Jay says generic SKiddies would be looking
for
hosts in general, which is true that time is a factor... My thoughts
are
that people and devices are getting smarter, and the old techniques
are
being changed.

So from what I understand of this thread:

- Is it good to allow icmp ping packets? --NO
- Is it good to allow UDP ping packets? --NO
- Do anything to slow down attackers! --Close and stealth all ports
that
you can. (which would prohibit the further scans from the utilities
that the
typical scripts and tools.)

BTW - I did find it very interesting with the earlier posts about
encapsulating Data within ICMP. (I wasn't aware)

Chris

My \$0.02 CDN

-----Original Message-----

From: Jay Woody [mailto:jay_woody@tnb.com]
Sent: Monday, September 08, 2003 11:12 AM
To: chatmaster@charter.net; Halverson, Chris
Cc: security-basics@securityfocus.com
Subject: RE: ICMP (Ping)

Guys again, I am not saying that you disable pings and walk away, job
done. If you do that, you are a moron. My point is that if you
disable
pings, that is ONE STEP in a myriad of stuff to do. Let's look at it
this way, if disabling pings stops one person and you have no need for
pings, then why not make it a step? Of course my argument is that it
stops way more than one person. Tim's argument is that it stops very
few. However, if it stops any, then some people would say it was
worth
it.

RE: ICMP (Ping)

SecurityFocus BASICS: RE: ICMP (Ping)

As an aside, Foundstone's tool is incredible. It zips up to around 300K and you guys are right, it port scans like a freaking demon. Still not as fast as pinging, but you guys are right the time is getting smaller and smaller.

I still believe that if someone was scanning an entire C range (or God forbid a B range), that they would prefer to whittle out the addresses that don't respond and not have to wait for the timeouts. You claim it did it all in 30 minutes, but maybe it would have timed out in 5 (just a wild guess). If you are scanning 255 addresses, that is over 21 hours of timeouts. All I am saying is that most of the tools will simply whittle out the ones that don't respond that way they don't have to wait for a timeout and then run something like this against them.

JayW

>>> "Halverson, Chris" <chris.halverson@encana.com> 09/08/03 11:13AM
>>>

I hate to say it but I do completely agree with Tim. If you get a free tool of superscan from FoundStone or most any other and you could scan an entire subnet for open services or ports that seem interesting in 30 minutes. Seeing a webservice that is open or a telnet port would allow most of them to zero in on that server. ICMP replies are usually irrelevant. I usually disable the service for the reason that when you are configuring Cisco Routers it is another access list command to enter.

Chris

-----Original Message-----

From: Tim Greer [mailto:chatmaster@charter.net]
Sent: Friday, September 05, 2003 4:40 PM
To: Jay Woody
Cc: security-basics@securityfocus.com
Subject: RE: ICMP (Ping)

On Fri, 2003-09-05 at 14:29, Jay Woody wrote:

> >> *What purpose would seeing a response from a ping serve to a
> >> kiddy looking to deface web sites? If they are going to attack
> >> you randomly, why do you assume that they would stop to
> >> think when they are blindly attacking networks/ips anyway?*
>
> *Here is how it works again.*

RE: ICMP (Ping)

SecurityFocus BASICS: RE: ICMP (Ping)

How what works? How you assume they will attack the network or probe it?

- > *They scan a range and then go back and run*
- > *a port scan/vuln scan against what replies.*

Most just simply run them. If they are up, they are up.

- > *They don't run vuln scans*
- > *randomly against ranges,*

Yes, actually, 'they' do.

- > *they run ping sweeps randomly against ranges,*
- > *those that reply get more attention.*

Not really. Some people may do that, but experience dictates otherwise. The people that randomly probe just do it, they don't make a list to spend a lot of time on unless it's an intentional, known target they have some desire to break into.

- > *So how would not replying help?*
- > *Well by getting less attention obviously.*

Why do you assume that out of millions of Ips that respond, one will get more attention than another? If you are correct and someone collects a list of "I'm live, I'm here" responding Ips are to later be targeted, that's one thing, but I've never seen that.

- > *They aren't "blindly*
- > *attacking networks/ips anyway". They are blindly scanning or sweeping*
- > *networks/ips through the use of pings.*

You assume so, but it's more likely a blind probing.

- > *They are not so blindly (but*
- > *almost) running a port scan those that reply. Then they are running*
- > *a*
- > *vuln scan against the boxes that just told them they were a certain*
- > *OS,*
- > *etc.*

Almost all scanners and worms even, will hit the range of IPs and not care if it responds to pings.

SecurityFocus BASICS: RE: ICMP (Ping)

> >> *Running a scanner to look for open ports of vulnerabilities*
> >> *in services, as not going to change because you don't reply*
> >> *to ping requests. Those scans will check the ports and*
> >> *services on said IP--not give up if it can't get a ping*
> >> *response.*
>
> *Man, dude, where do I start on this one? :) Yes, running something*
> *like that would behave exactly as you describe (I think). However,*
that
> *isn't at all what anyone has said. Again, they "scan" the ADDRESSES*
in
> *a range for a simple reply and then run a port scan/vuln scan*
against
> *those that reply.*

> *From what I've seen, that's not the case. They don't first check to*
see
that it's alive, they can see it's alive without waiting for a ping
response. They will most likely initially scan for common services to
see if it's alive. Not only is it more accurate, but it's also
telling
them that the service they want to test is up.

> *Your point is that if they don't respond to pings,*
> *they likely won't respond to vuln scans.*

No, I didn't say that.

> *The script kiddies say the*
> *same thing in reverse.*

Huh? That's what I said. I said that will scan it, not caring if it
replies from a ping request.

> *If you respond to a ping you likely will give up*
> *more information if asked.*

But less helpful information than you would getting a response from a
service you are looking for being up. Hence, ping is irrelevant, they
will hit the ports/services to see if they should "come back".

> *Again, they scan the range for replies and*
> *then run a port scan/vuln scan against the replies for more info.*

They do? How do you know this? How do you know that's what most or
all
of the script kiddies do?

> *They*
> *don't blindly run a vuln scan against a range. That would be even*
more

RE: ICMP (Ping)

SecurityFocus BASICS: RE: ICMP (Ping)

> *stupid and waste time.*

Uh, we're talking about random scans/probing and script kiddies and you think that's unlikely because it would be 'stupid'? This is why script kiddies are a joke and why ping responses are not going to make a difference.

> >> *And that doesn't relate to the type of attacks being discussed. That's another, less serious issue anyway.*
>
> *Uh, OK.*

Indeed.

> *The question was should your devices reply.*

Yes, that was the question.

> *There is not an ATTACK there.*

No, there's certainly not.

> *The statement was that no, they shouldn't because then you get more interest from the kiddies.*

Not really, but you don't have to share my opinion nor belief.

> *You said no you don't and I said yes you do.*

Yes, that's correct.. that appears to be what we said.

> *Haven't heard about any attack mentioned at all.*

Haven't you been reading what I said?

> *Also, if you think having your web page defaced is not serious, then ask Nike how much the press hurt them and ask Microsoft how much money they spend on making sure it doesn't happen to them.*

Who is their lack of security an issue when it comes to how much 'attention' a ping response will get you or not? I don't believe it will, because random scans will randomly scan you anyway. I've disabled ICMP for ping requests on different networks and I see the same amount of probing/scanning activity on them as one's with it enabled. As for

RE: ICMP (Ping)

SecurityFocus BASICS: RE: ICMP (Ping)

Nike and MS, they are targets, it has no bearing on them responding to ping requests.

> *If you are a seller,*
> *then having your web page defaced and pointing people to a site that*
> *gathers their credit card numbers would be decently serious I would*
> *think.*

Ping responses have absolutely no bearing on the security of your server/web site. It's either secure or it's not. You have the opinion that someone's going to randomly ping Ip's looking for responses, rather than simply seeing if a service is running, is going to save some people from being compromised. I disagree. If your security is so slack that a script kiddie can later come back simply from seeing the IP was pingable, then you have bigger concerns than ping responses to worry about. Also, consider this; if you have someone skilled enough to have any chance of getting into most servers, those will not likely be the type of people that will think a ping response means anything and, instead, they will be scanning for open ports/services. No, ping doesn't hide you.

> > *No, they'd probe for vulnerabilities by domain or IP, the*
> > *ping response plays no role in that situation.*
>
> *If they are probing for vulnerabilities by domain (and I am not 100%*
> *sure what you mean there), then they are retarded.*

That depends on how you look at it. They may have specific types of sites that they want to compromise. Grabbing a list of domains (ie., from an old whois db) would serve up all the domains with 'shop' in them, for example. Either way, someone's that's going to randomly scan IP ranges with no target in mind, is retarded anyway. I don't know about you, but I don't worry about those type.

> *I said that they*
> *deface the web page and move on and you reply that they scan for*
> *vulns*
> *by domain.*

Pings have nothing to do with web site defacement. Poor security does.

How someone finds them, is irrelevant. Lack of a ping response doesn't hide you.

RE: ICMP (Ping)

SecurityFocus BASICS: RE: ICMP (Ping)

> *Again, the ping response plays a HUGE role.*

I disagree.

> *They ping a*

> *group of addresses, if you don't respond they move the FREAK ON.*

Unless they just happen to test for more accurate results, which a skilled enough cracker to be a threat would be doing anyway.

> *If you*

> *do, they run a port scan, then a vuln scan against you.*

Or they just do anyway, since we're talking about retards.

> *By not*

> *replying, you stop the kiddies from looking (in addition to many of the*

> *other DDoS issues mentioned already).*

You're living in a dream world if you really think you saying this makes

it true. As for some types of attacks, I stated, depending on what protocol, it couldn't hurt and may help minimize damage. As for site defacers and people looking to crack your box, forget it, it makes absolutely no difference.

> *"[T]hey'd probe for*

> *vulnerabilities . . . IP", yep, exactly and where did they get the IP*

> *address?*

Where exactly do you think they get the IP to ping in the first place?

They hit it and see. Instead of hitting it for an unhelpful ping response, they hit services or ports and see if it's up and a potential

target. Responding to pings doesn't make you a target.

> *By the freaking ping reply.*

Like I said, how do you imagine they get those IP's to try and get a ping response from? What is this, a joke?

> *No reply, less attempts.*

In your opinion, you a

> *I am*

> *just not saying it right or something, so help me see where we are*

> *missing it.*

RE: ICMP (Ping)

SecurityFocus BASICS: RE: ICMP (Ping)

I've been trying.

- > >> *That is irrelevant.*
- >
- > *Then your point is irrelevant,*

No.

- > *because I was agreeing with your point.*

No, you weren't. Read the responses.

- > *Sure, some people see a site and say, "I want to hack that particular*
- > *company." 99% don't.*

And those 99% will scan for services being up, not give up on a lack of a ping response—that means nothing.

- > *They say, I want to hack 40 sites in a week. I*
- > *don't give a crap who, so let's see who replies.*

And they'll start scanning ports/services.

- > >> *True. You're either vulnerable or not. But it depends on the*
- > >> *type of attack and on what service or protocol.*
- >
- > *And if you don't reply to pings then 90% of the kiddies never even*
- try
- > *to find out what will work against you.*

No. Refer to above.

- >
- > >> *No it doesn't. Skripties are stupid by nature. They hit*
- > >> *blindly with the scanners, the scanners don't give up if*
- > >> *there's no ping response,*
- >
- > *See, here is where you keep missing it.*

This is ironic. Do I need to explain?

- > *They DO NOT blindly run vuln*
- > *scans.*

Says who? Says you? Why are you so certain people will check for a measly, means nothing ping response, instead of just testing fir a response on a common port, like port 80—after all, they are after web servers. Just because you say it, doesn't make it so.

RE: ICMP (Ping)

SecurityFocus BASICS: RE: ICMP (Ping)

> *They blindly run Ping sweeps.*

There's no rule to say that's what they *_must_* do and, again, in my experience, that's not the case. Are you more worried about the people that think they need to ping a server to think something's there, or the more thoughtful cracker whom checks to see if you have services running, because they know pings don't matter? So, your entire point and reasoning therefore, is that you can do this to prevent the most clueless script kiddies that use the most suckiest tool/scanner, from trying to deface your web site? Does that really worry you... at all?

> *They scan a range and see who*
> *replies*

I'm sure you're familiar with the term "middle man" and 'cutting them out'? Why would they do this, when they can simply check to see if you have a specific service listening on its port?

> *and then they run the port scan that you describe against just*
> *those areas that replied.*

I suppose that they could. Sounds like double the work. I'm not worried about the people that are literally that stupid—to be doing double the work. You should be worried about the more skilled people, if any.

> *Then they run the vuln scan against just*
> *those addressed that replied and that have a certain OS, etc.*

And they can do this without the delay.

> *That is*
> *well known.*

And my examples of why this doesn't matter are valid.

> *So either you are saying they run vuln scans against huge*
> *ranges,*

Yes, the idiots that think a ping response means anything useful, will indeed be stupid enough to just let it rip and scan ip ranges. It has the same effect anyway—if something is there, it's there. If it's not, it's not and their scan will skip it or move on. They randomly scan ip ranges to compile a list of servers that are running certain services, not just see what IP's respond. That's pointless.

RE: ICMP (Ping)

SecurityFocus BASICS: RE: ICMP (Ping)

> *which isn't true*

It is true. Try and deal with it.

> *or you are saying that ping sweeps or scans*

> *will still document you when you don't reply, which is also not true.*

Okay, so you're claiming that it's not true that scans on port 80 to see if there's a web server aren't purposeful (or even more so) than just seeing if the IP responds?

> *They don't run an in depth scan until they see if you are alive or not.*

Who said it had to be in-depth? They can check for even only one relevant service, like a web server—since they are defacing web sites (or intending to). Which is more valuable? A response saying the server is up, or the server is up and running a web server? Why is this so difficult to fathom?

> *If you are not alive, why waste their time,*

But that's just it, no one cares if the IP responds saying it's alive or not. It is just as quick and more logical and efficient to just straight out check and see if a service is up.

> *there are plenty of people*

> *that are.*

Yes, that's right. Script kiddies likely waste a lot of time... like compiling a list of IPs that are alive at that very time, which means nothing.

> *I run Zone Alarm at home.*

Okay, I won't ask why you do.

> *They ping me and I don't reply,*

So?

> *now they could run a suite of vuln scans against me and an hour or more*

> *to see what is turned up OR they could move to next door neighbors PC*

> *where the password is password.*

RE: ICMP (Ping)

SecurityFocus BASICS: RE: ICMP (Ping)

Or, they can see if you're a server running a web service and mock you about how you thought they'd have moved on because you didn't respond to silly little ping requests. I'm honestly not saying this to insult you, but I don't see how you can argue the point... perhaps you just think the same about me and my points. Oh well.

> *They just move on.*

Or so you assume.

> *They are looking*

> *for the slow, stupid ones on the fringe to gobble up.*

So, you're saying people that don't drop ping responses are stupid? Odd, I've only disabled responses on maybe 5 servers in the last 8 years and I've never been compromised... it must not be the ping factor at play.

> *If you don't*

> *reply to a ping, most script kiddies will simply move on.*

I think the better question is, who would worry about such script kiddies that use those tactics anyway? I mean, you do secure your servers and network, right?

> *That has been*

> *the opinion espoused by a great majority of responders to this thread,*

> *so I am obviously not the only one that feels this way.*

Hey, there's nothing wrong with doing this in my opinion, I just don't see the point to use it in any way at all to prevent being attacked or your system compromised.

> > *they are busy checking to see what's running on the various*

> > *ports that particular scanner scans. It's almost contradictory*

> > *to use script kiddie and 'dig deeper' in the same sentence.*

>

> *Not if you didn't reply to a ping they don't.*

Fine, don't read any single thing I said. I am tired of repeating myself.

> *Think about it man.*

Irony...

SecurityFocus BASICS: RE: ICMP (Ping)

> *If*
> *you ping sweep a range of 255 addresses and 20 respond and you are a*
> *little kiddie, you are going to focus on those 20, crack 5 quickly*
and
> *go brag about it.*

Maybe those 20 servers should have been secured at some point, would
be
my question? I'd demand to know how someone could be so incompetent
to
get cracked by a script kiddie.

> *You are not going to kick off your favorite little*
> *vuln scanner against addresses that "aren't up"*

Sure you are... maybe you aren't, but enough do.

> *in the hopes that maybe*
> *one is, spend all night dicking with that one and then having*
nothing
to
> *brag about.*

Or, like I said, they actually look for one's that are targets, seeing
if they are running a service, not just alive. Oh, I've explained
this
to death.

> *It is a numbers game. They want to be able to say they*
> *cracked X number last night.*

So having the middle man, rather than just checking to see if a
service
is up makes their task faster somehow? How's that?

> *Not that they spent all night scanning a*
> *range and then finding out that indeed there really were no other*
boxes
> *there.*

And the scanner moves on if there's no service they are targeting,
just
as it would if there was no ping response—but is more accurate.

> > *But they aren't looking for boxes that reply to ping requests,*
> > *they hit the IP on various ports to check to see if that port/*
> > *service responds and with what.*
>
> *I am beginning to think you are screwing with me now.*

I know the feeling.

RE: ICMP (Ping)

SecurityFocus BASICS: RE: ICMP (Ping)

- > *Surely you have*
- > *downloaded one of these things.*

How is that relevant? I could code a script to check for the 5 common services on a server and iterate through however large of an ip range

I wanted and just collect a list to hit... why the heck would I care about pings responding?

- > *They don't do that at all.*

You should find a better source for your script kiddie tools then.

- > *They first*
- > *sweep a range and gather addresses.*

Perhaps if they are using the most lame tool around?

- > *Then they compile that in a list.*

Why not compile a list of systems actually running a service you are targeting?

- > *Then they run their port scan/vuln scan against each of those IPs*
- and
- > *THAT scanner is what looks for ports, weak passwords, etc.*

I know what you're saying.. you're saying "You can waste all night on one server that may not be there, so they first check for a response."

As logical as that may sound to you, the method of scanning for the relevant services is just as quick as checking for a ping response.

If there's no services up that you're targeting, you move on...

- > *The point*
- > *being made here, over and over, is that if you are not one of the*
- > *addresses on the list, then the scanner isn't run against you.*

My point being; If they use that sort of scanner and strategy. Most don't from my years of experience auditing logs. Also, the fact that who cares about these fools, secure your system and don't worry about it. And, finally, that the one's skilled enough to even have a chance will have either targeted you to be interested in the first place, OR, they will use a more accurate method to compile a list of IPs that are running actual relevant services.

Random scans for live IPs doesn't equate to the person wasting their time trying every possible exploit on the IP—they will still check for

SecurityFocus BASICS: RE: ICMP (Ping)

the common services and vulnerabilities. As you said yourself, the goofs want to move on, they aren't going to do an in-depth scan of a server that isn't going to give up root soon anyway by your logic.

And,
with a secured server, who cares about these idiots?

> *How do
you stay off of the list?*

Why do I care if I'm on it?

> *Well, how did you get on it?*

By not worrying about irrelevant things and feeling safe about something so trivial?

> *You responded
to a ping.*

Okay, I'm not worried, why are you?

> *No response equals less kiddie attacks.*

So? These are the people you'd be worried about?

> *Period.*

In your opinion, my experience dictates differently. Perhaps yours is not the same.

> *Less
script kiddie attacks means more time to get the vulns patched and less
of a chance that a bonehead move gets you compromised.*

No script kiddie that lame is going to get into a server anyway. That's all there is to it. A script kiddie smart enough to try with a 0-day exploit wouldn't have a chance if they were tat random about it anyway.

They'd try the exploit through IPs, not make a lost to try... it would have the same result. If they can't figure that out, they aren't a threat.

> > *Like I said, a dumb ass script kiddie will hit the ports
> > checking the services for vulnerable services. Ping
> > response or not makes absolutely no difference.
>
> And like I said, it absolutely does.*

RE: ICMP (Ping)

SecurityFocus BASICS: RE: ICMP (Ping)

Fine, we can disagree.

- > *They are not doing random port*
- > *scans.*

They are, they will and they do.

- > *They are doing random PING SWEEPS and then doing semi-random*
- > *port scans on those that REPLY.*

I'm sure that *_some_* are, sure.

- > *Then running specific vuln scans on*
- > *boxes that replied as needed to the port scans.*

If they think it's a viable target, sure. However, a ping response or not, will not be what determines how much time they want to waste. So, a ping response or just cutting the middle man out of the picture and checking for relevant services... either way, it makes no difference. If you're vulnerable, you get 'got'. End of story.

- > *You seem to think they*
- > *just jump right into the port scanning world and they just don't.*

I tend to think they do, because that's the nature of the script kiddie. If they use the method you outlined, so be it... either way, there's enough out there that do, so this makes no difference and will only matter if you are vulnerable anyway.

- > *Why*
- > *run a port scan against a non-existent box?*

Why check for a ping response from a non-existent box?

- > *It is just a waste of your*
- > *time.*

Sort of like compiling a list of live IPs for no damn good reason.

- > *They don't.*

They do.

- >
- > >> *It's either going to happen or not, random or targeted.*
- > >> *If it's random, you'll be hit and probed anyway (being an*
- > >> *attach or probe). If it's not random, well, we all know the*
- > >> *answer.*
- >
- > *If they were running port scans, you might be right,*

RE: ICMP (Ping)

SecurityFocus BASICS: RE: ICMP (Ping)

They do, they are, they will. Of course some don't, some will use the strategy you outlined. Those would be the less skilled, why worry.

- > *but again, they*
- > *don't until*

No, that's a condition you added. Many do. Speak specifically in terms of the one's that don't to make your point, don't act like none do or would—it happens all day, all the time, on tens of thousands of networks, in fact.

- > *you first let them know there is a box there to run one*
- > *against.*

If they use the method you outlined, sure. If they don, all bets are off.

- > *No box, no port scan.*

In your mind.

- > *No ping, no box to them. On to the*
- > *next range.*

In your mind.

- > >> *I don't see the point to that side of this debate.*
- >
- > *Cause you aren't trying.*

Oh, if you say so. :-)

- > *You are just insisting that the process*
- > *starts in the middle.*

No, I'm insisting that people don't have any reason to have a middle man, so they don't.

- > *It doesn't.*

It "do".

- > *It starts at the beginning and that*
- > *is the ping sweep.*

You are instant about that, for what reason, I can't imagine. Wake up.

- > *If I were you, I would try to understand that side*
- > *seeing as how a great majority of the posters have thus far espoused*

RE: ICMP (Ping)

SecurityFocus BASICS: RE: ICMP (Ping)

the

> *same idea.*

No, they stated they disable it for other reasons, not because they think it's a good rock to hide under. My points are true and valid. Some script kiddies may use that method, sure, but a lot do not. The more skilled one's are the one's that do not.

> *You seem to be under the impression that a kiddie's first tool is his port scanner and it isn't.*

Well, I guess I wouldn't know, I won't argue with your experience. I simple outlined mine.

> *It is his ping sweeper.*

Well, if you say so... you have, and continue to... even though it makes no difference.

> *THAT produces the list that he uses for everything else.*

Sure, whatever.

> *Again, not 100% of the time, but 90-95% of it.*

I'm not sure what you mean by that, sounds like you're saying even that doesn't matter to the people that use that method, which seems silly.

> *My 2 cents. Maybe that clarifies it.*

Not really. But it doesn't matter.

--

Tim Greer <chatmaster@charter.net>

Attend Black Hat Briefings & Training Federal, September 29-30 (Training), October 1-2 (Briefings) in Tysons Corner, VA; the world's premier technical IT security event. Modeled after the famous Black Hat event in Las Vegas! 6 tracks, 12 training sessions, top speakers and sponsors. Symantec is the Diamond sponsor. Early-bird registration ends September 6. Visit us: www.blackhat.com

Captus Networks
Are you prepared for the next Sobig & Blaster?
- Instantly Stop DoS/DDoS Attacks, Worms & Port Scans
- Precisely Define and Implement Network Security

RE: ICMP (Ping)

SecurityFocus BASICS: RE: ICMP (Ping)

- Automatically Control P2P, IM and Spam Traffic
FIND OUT NOW - FREE Vulnerability Assessment Toolkit
<http://www.captusnetworks.com/ads/42.htm>
