

Re: [Full-disclosure] [Professional IT Security Providers -Exposed] PlanNetGroup ( F )

## Re: [Full-disclosure] [Professional IT Security Providers -Exposed] PlanNetGroup ( F )

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2008-01/msg00407.html>

---

- *From:* "Jerry dePriest" <jerryde@xxxxxx>
  - *Date:* Mon, 21 Jan 2008 10:55:41 -0600
- 

nice to see some have mlk off and nothing better to do

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

*From:* "SecReview" <secreview@xxxxxxxxxxxx>

*To:* <nate.mcfeters@xxxxxxxx>

*Cc:* <full-disclosure@xxxxxxxxxxxxxxxx>

*Sent:* Monday, January 21, 2008 10:40 AM

*Subject:* Re: [Full-disclosure] [Professional IT Security Providers -Exposed] PlanNetGroup ( F )

Nate,

Your email was constructive and much appreciated. We'll go over the review a second time and incorporate some of your suggestions. Thank you for taking the time to provide so much good feedback.

On Mon, 21 Jan 2008 02:07:50 -0500 Nate McFeters <nate.mcfeters@xxxxxxxx> wrote:

SecReview,

My 2 cents on your review, although I will try to be nicer than you were to the reviewee. I'm completely skipping your section where you talked to the non-technical person, that's not even fair... sorta like reviewing a consulting group based on their website alone... oh shit, I forgot you guys do that too.

Your comments on Question 1:

We're not impressed with Michael's answer. First off we have no idea what the hell this means: "Depending on time and availability, we will work on

Re: [Full-disclosure] [Professional IT Security Providers –Exposed] PlanNetGroup ( F )

finding any new vulnerability if we generate an anomaly of interest." And we totally disagree with "Currently, the focus is primarily on discovering new Oracle vulnerabilities – as MS SQL 2K5 is more difficult to beat on, compared to Oracle." In fact, whatever is being described above doesn't sound anything like a vulnerability assessment, we're not sure what kind of service it is.

The first portion "Depending on time and availability..." I don't understand what your confusion is. Basically the responder is saying that he's willing to do what the client will pay him for. Consulting is not a cookie-cutter gig, so sometimes clients want you to spend 5 minutes running scans, some want you to fuzz a proprietary protocol for as long as it takes. I personally don't think either end of the extreme is of value to the client, but you can hardly fault the respondent for delivering what the client asks for.

The second, I don't agree the overall focus is on Oracle, but if you read the new (ZDnet, eWeek), or if you follow the conferences (HITB Malaysia 2007 great Oracle presentation), then you will know that Oracle is catching a bit of the limelight. Besides that, I don't think you are qualified to say what exactly a vulnerability assessment is... if the client is paying you to assess their database servers, then that is a vulnerability assessment of their database servers and that is what the work is. Different clients have different needs, and there are different specialty consulting groups to help meet those... can hardly fault him if his specialty is databases.

Your Comments on Question 2:

trying to be cute with your "Again, carefully!" bullshit?

Come on guys... imagine you get called by a group of people asking to assess your company and you don't know who they are, wouldn't you try to befriend them if possible? A little professionalism would go a long way to improving your reviews.

A penetration test is not "Anything Goes!"

Umm... sorry guys, there is plenty of cause for performing a Denial of Service test. Keep in mind that availability is a large portion of what security is about. I don't think he's talking about using a bot net to try to take them down.

it doesn't sound like Michael knows how to perform IDS evasion

testing.  
Using a proxy is >>not going to help anyone evade detection, it will just help them to hide their IP address.

Hmm... well, you're partially right. I suppose that if he had enough proxy servers and kept his scans very focused, he "might" be able to get around an IDS. In any case, not all clients want IDS evasion performed... for instance, they may want to test their incident response, or, they may allow the consulting group through the IPS/IDS in an effort to save on time and costs.

Your response to question 3:

From the answer above, it looks like they like the same tools as

most people. That said, >>we've seen no proof of talent from anyone at PlanNetGroup yet. So we're near certain that >>their deliverables

ARE the  
product of automation.

If they are the same tools that everyone use, how can you knock them for that? It seems to me that a group starts with a score of 0 in your book, and then if they impress you they get points. If you don't ask the right questions, I don't see how they could impress you. I concede, it is certainly possible that they have no skills, and that they use automation, but I don't think it is fair to say that at this point of the review.

Your response to question 4:

Woha, it takes too much time to create a fake deliverable? Well

that's one way to get out >>of it, but we don't buy it. Either way, at this point we don't feel that a sample report would >>help this review, we've seen nothing impressive yet.

Ever tried to do so? It does take awhile, and it is risky. If you miss sanitization and release results of one of your clients you could get sued. Perhaps given the context of the investigation he didn't want to give you an old report and it would take to long and too much of his billable time to actually get this to you. That's not unreasonable. You aren't paying him. Again with the comments of nothing impressive yet. You are asking generic questions, how could anything be impressive? It's a phone call or email and you are asking questions that almost all consulting groups should have relatively the same answers to... I see nothing impressive in that at all.

Your response to question 5:

It sounds like Michael has a difficult time sticking to the

scope of work.

Any time anyone >>performs Distributed Metastasis it should be built into a scope of work first. If it is not, >>then do not perform the testing because it is invasive and will get you into trouble. This is >>a big negative point in our eyes as its critical that providers are able to adhere to the scope

of work for each specific engagement.

I actually agree with most of this, but then again, as long as he doesn't go over the clients budgetary and time constraints and is providing the customer with value, I have no problem with going outside of scope as long as the client does not. Also, I don't know that it is a big negative as you say.

Your response to question 6:

It sounds like Michael is a corporate security guy and has no

experience as a hacker.

Bit of a blanket statement I'd say, but OK, let's assume you are correct

Certifications hold little to no water when it comes to real IT

security.

Agreed, but you are totally putting words into his mouth. He basically says the same thing by calling the CISSP a definition test. Why do that? Most people in security have the certs... most realize they are worth nothing and don't really test tech knowledge, but instead test business knowledge.

What does hold water is experience and  
from what we can tell,

Michael has  
no real hacker >>experience.  
Please define "no real hacker experience". If you mean he isn't  
31337 like  
you guys, then OK. BTW, most clients aren't just paying for "real  
hacker  
experience" they're also paying for the business side, i.e. what  
is my risk,  
how can I mitigate, etc. A good team has both people.

On your response to question 7:

Do you resell third party technologies?

We don't think that it is a good idea that  
Professional IT

Security  
Providers sell third party >>technologies. Specifically because  
they become  
biased towards a specific technology and >>push that technology as  
a method  
of remediation when better methods might already exist.  
Agreed. But that said, what if your third-party tech. has nothing  
to do  
with the main thrust of your consulting work? The question is  
pretty vague.

On your response to question 8 and 9:

Ok, I'll buy that you have cookie cutter definitions from google  
of those  
flaws and that his definitions don't fit. I'll even buy that you  
make a  
good point when you say EIP overwrite is not the only method of  
exploitation  
(especially these days), but I'm wondering what you expected.  
Should he  
have rattled on and on about how to exploit b0f in an XP SP 2  
environment?  
Talk to you at length about DEP? Bit ridiculous expectations.  
Hell, while  
your at it, why didn't you ask him about integer overflows? Off-  
by  
one/few/many exploits? Heap overflows? Why not have him recite  
the Heap  
Fung Sheui method to you? What about double free flaws, dangling

Re: [Full-disclosure] [Professional IT Security Providers –Exposed] PlanNetGroup ( F )

pointers,  
etc. etc. etc. Let's be serious here, unless you are contracted  
by  
Microsoft or another major software vendor, you probably don't pay  
the bills  
by doing your own research, so... does this really matter? Sure,  
it's  
great... I'd like to know that consultants I was paying top dollar  
to knew  
about this, but if he comes on site and spends 3 weeks trying to  
find an  
integer overflow, I'm going to be pissed.

Disclaimer:

I'm not a client of PlanNetGroup. Also, I don't think what you  
are trying  
to do is a terrible thing, there's lots of snake oil being sold in  
the  
commoditized security market out there, but I disapprove of your  
professionalism and your methods. Also, I believe the list is  
still waiting  
for you to credentialize yourself/yourselves. That still hasn't  
seem to be  
grasped here. Look, if you're someone people respect, then maybe  
people  
will buy your reviews, but somehow I doubt that is the case. I'm  
basing  
that view off of the content of your website and the fact that you  
still  
have not credentialized yourself as the list called for so long  
ago. Do  
that, and I will re-review my review of your reviews.

Nate

On Jan 20, 2008 7:17 PM, secreview <secreview@xxxxxxxxxxxx> wrote:

The PlanNetGroup is a Professional IT Security Services  
Provider

located

at <http://www.plannetgroup.com>.  
<<http://www.plannetgroup.com>>

One of our

readers requested that we perform a review of the  
PlanNetGroup,

so here it

is. It is important to state that there isn't all that much

information

available on the web about the PlanNetGroup, so this review is

based mostly

on the interviews that we performed.

The PlanNetGroup was founded by Jim Mazotas of Ohio USA

according to this Affirmative

Action Verification  
Form<<http://odnapps01.odn.state.oh.us/das->

eod/EODBMSDev.nsf/d881c0c739c3c9b985257344004f1929/c3e323de1df5162b8525735d00607a6d?OpenDocument>.

We called Mr. Succotash and spoke with him for about an hour

about his

company, here's what he had to say.

When we spoke with Jim Mazotas we asked him how he defined a

Penetration

Test. His answer wasn't really an answer at all but rather was a

bunch of

technical words strung into sentences that made no sense. Here

is what he

said for the most part. We can't give you an exact quote because

he

Re: [Full-disclosure] [Professional IT Security Providers –Exposed] PlanNetGroup ( F )

requested that some of the information related to clients, etc  
be kept  
confidential.

"We get to target object, where we go with that is based upon  
the client's

comfort level. We grab banner information, backend support  
information, and

other kinds of information. During a penetration test we most  
will not

penetrate. Most mid level companies will not want  
penetration."

Sanitized

Quote from Jim

Not only do we not understand what Jim said, but he'd be  
better

off saying

"I don't know" next time instead of looking like an idiot and  
making up an

answer. This goes for all of you people that get asked  
technical

questions.

If you say "I don't know" at least you won't look like a fool.

Anyway.

When we asked Jim to define a Vulnerability Assessment,  
we

became even

more flustered. Again his answer was like a politician trying  
to

evade a

question with a bunch of nonsensical noise. Again, we've

sanitized this at

Jim's request.

" A Vulnerability Assessment is more a lab based environment

type test.

Analyze servers and all nodes that are a true vital asset to the

company and

assess the vulnerability In a very planned out manner. This is

done in a lab

based environment." Sanitized Quote from Jim

Again, next time say "I don't know" because now you look like an

idiot.

Nobody expects you to know everything, but when you make shit up

and try to

fool people, its insulting. To be fair to Jim, he did say that

he was not

technical, but we didn't get technical here. As the founder of

the business

he should at least know what his different service boundaries

are and how

his services are defined.

When we asked Jim if his team performed Vulnerability Research

and

Development, he said that they did not have the time because they were

"fully booked". His primary customer base includes state government and a

few private sector businesses. Unfortunately, we can't disclose

who his

exact customers are. He did say that he provides Network Management Services

and Wireless Management services for many of his clients. Sounds

more IT

related than Professional Security related.

When we finished with our call to Jim we asked him if he'd be

kind enough

to give us contact information for someone more technical in his

company. He

told us that he'd be happy to arrange a call with someone. At

the end, we

didn't end up calling anyone but instead shot a few emails back

and fourth.

The rest of this review is based on those emails.

We decided to ask the same questions to Jim's technical expert.

We know

Re: [Full-disclosure] [Professional IT Security Providers –Exposed] PlanNetGroup ( F )

who his expert is, but we assume that he wants to stay anonymous

because he

signed his email with "Jason Bourne". So for the sake of this

interview

we'll call him Michael. Here's the email from Michael:

–) How do you perform your vulnerability assessments?

"\* Carefully! :) Typically, we will work with the customer to

define the

scope of the assessment; limitations to OS, Network Equipment,

Web

Server, etc. This could be a combination of components

(depending on

scope), the real goal ultimately with this is to assess the

patching

effort of a customer. Depending on time and availability, we

will work

on finding any new vulnerability if we generate an anomaly of

interest.

Currently, the focus is primarily on discovering new Oracle vulnerabilities – as MS SQL 2K5 is more difficult to beat on,

compared

to Oracle. Within vulnerability assessments, we disregard any

attempts

to evade IDS, IPS, etc."

Re: [Full-disclosure] [Professional IT Security Providers –Exposed] PlanNetGroup ( F )

Re: [Full-disclosure] [Professional IT Security Providers –Exposed] PlanNetGroup ( F )

We're not impressed with Michael's answer. First off we have no

idea what

the hell this means: "Depending on time and availability, we

will work on

finding any new vulnerability if we generate an anomaly of

interest." And we

totally disagree with "Currently, the focus is primarily on

discovering new

Oracle vulnerabilities – as MS SQL 2K5 is more difficult to beat

on,

compared to Oracle." In fact, whatever is being described above

doesn't

sound anything like a vulnerability assessment, we're not sure

what kind of

service it is.

–) How do you perform your penetration testing?

\* Again, carefully! The definition that I use with customers is –

Anything Goes! In addition to attempting to locate missing

patches,

vulnerable IOS's, applications, etc – we will perform an

assortment of

timed attacks, attempt to spoof trusted connections, or even

perform

social engineering – like dropping a few pre-trojan'd usb data

sticks

outside of a customer service area, a data center, etc. The only

thing

that we do not perform, typically, is denial of service style or

type of

attacks. We have had only one customer that we felt was in the

position

to handle such a test and it was performed against their

disaster

recovery infrastructure, not production."

Michael, why are you trying to be cute with your "Again, carefully!"

bullshit? A penetration test is not "Anything Goes!", if that's

how you

define it then I don't want you anywhere near any of my

networks. And why

the hell would you perform a Denial of Service attack against

anyone?

Everybody can be knocked off line if you fill up their pipe. You

scare us

man!

Re: [Full-disclosure] [Professional IT Security Providers –Exposed] PlanNetGroup ( F )

–) How do you perform evasive IDS testing?

"\* We use a series of proxy servers to attempt to perform basic

hacking

techniques; port scans, blatant attacks, etc. We are typically

going to

look for TCP resets as a means to evaluate if IDS is present and possibly to find if IDS performs blocking activity. Often times,

if a

system in a trusted DMZ can be compromised and used as a proxy (exploiting a relationship or rule within a firewall) or an SSH,

SSL,

encrypted tunnel can be established to a server behind the IDS

sensor

than we can successfully pull off an attack without the

customers

security staff even knowing."

It doesn't sound like Michael knows how to perform IDS evasion

testing.

Using a proxy is not going to help anyone evade detection, it

will just help

them to hide their IP address. If the target network or

application is being

protected by an IPS device, then the IP that they are attacking

Re: [Full-disclosure] [Professional IT Security Providers –Exposed] PlanNetGroup ( F )

from will be

shunned just the same. So, we understand that the  
PlanNetGroup's

expert

hasn't a clue as to how to evade IDS. (Michael, did you get  
your

answer from

Google?)

–) What tools do you favor?

"\* We really do not favor any tools. The focus of our effort

(Assuming we

are performing a pen-test or assessment) is to analyze a

situation and

choose the best tool for the end result or compromise. I will

use commercial

applications, such as AppScan, WebInspect, even ISS. There  
are

however

plenty of freeware, low-cost tools that we use; nmap, nessus,

metasploit –

ultimately, I find that an internet browser and a telnet prompt

will suffice

for much of the testing. It ultimately gets back to interpreting

the results

and adjusting the testing accordingly. We make it a point to  
try

out new

Re: [Full-disclosure] [Professional IT Security Providers –Exposed] PlanNetGroup ( F )

freeware tools on every assignment. The more tools that we know

of and can

test with opens our options if in the future a situation best

suited for a

tool presents itself."

Every business that delivers security services has a set of

tools that

they use. These tools change from business to business, but

common ones are

nessus, webinspect, CANVAS, Core Impact, Metasploit, etc. From

the answer

above, it looks like they like the same tools as most people.

That said,

we've seen no proof of talent from anyone at PlanNetGroup yet.

So we're near

certain that their deliverables ARE the product of automation.

–) Can you provide us with sample deliverables? (sanitized)

"\* No, too much time. Even to sanitize creates an opportunity

for a

liability in the event that a customer name is exposed ...

accidents do

happen! I will say that we do not take dumps from applications

and

Re: [Full-disclosure] [Professional IT Security Providers –Exposed] PlanNetGroup ( F )

Re: [Full-disclosure] [Professional IT Security Providers –Exposed] PlanNetGroup ( F )

regurgitations the information on paper. We limit our executive

summary to 6

pages at most and attempt to keep the entire report limited to

25 pages in

total. Our goal with a deliverable is to get the precise

information to the

key stake holders so that they can make a decision."

Woha, it takes too much time to create a fake deliverable?  
Well

that's one

way to get out of it, but we don't buy it. Either way, at this

point we

don't feel that a sample report would help this review, we've

seen nothing

impressive yet.

–) Do you offer the option of performing Distributed  
Metastasis?

"\* No, not really. This is my decision as in a previous life I

got walked

out of Bell Atlantic Mobile (Verizon Wireless) using this

technique when I

compromised their Unix infrastructure by compromising the  
rlogin

function

(on all Unix servers, across all data centers). There is no

substitute for

Re: [Full-disclosure] [Professional IT Security Providers –Exposed] PlanNetGroup ( F )

experience, especially bad ones!"

It sounds like Michael has a difficult time sticking to the scope of work.

Any time anyone performs Distributed Metastasis it should be

built into a

scope of work first. If it is not, then do not perform the testing because

it is invasive and will get you into trouble. This is a big negative point

in our eyes as its critical that providers are able to adhere to the scope

of work for each specific engagement.

–) What is your background with relation to information security?

"\* Too long, too boring. Yeah got the CISSP (nice vocabulary

test), but

had to as I worked for DOD. Got a number of Certifications (I

have a stack

almost an inch thick and only get into them about once a year to

throw

another couple on top of the previous ones – too much alphabet

soup for me,

but bosses and customers like it. Spoke at a number of European conferences, but found too many people did not

understand a word

I was talking about, so I got tired of that and quit that scene.

My outlook

on security has changed, to the point that I will advise

customers of their

risk, attempt to make it practical – but if they make a

conscious choice not

to listen – I do not fret over it.?"

It sounds like Michael is a corporate security guy and has no

experience

as a hacker. Certifications hold little to no water when it

comes to real IT

security. What does hold water is experience and from what we

can tell,

Michael has no real hacker experience.

–) Do you resell third party technologies?

"\* No, but kind of wished that we would. I think that it would

help with

sales."

We don't think that it is a good idea that Professional IT

Security

Providers sell third party technologies. Specifically because

they become

biased towards a specific technology and push that technology as

a method of

remediation when better methods might already exist.

–) Can you tell me why the EIP is important?

"\* The EIP controls an applications execution. If an attacker can modify

the EIP while it is being pushed on the stack then the attacker

\*could\*

execute their own code and create a thread (aka. a buffer

overflow condition

exists). I had a good refresher this past year at Blackhat with

a course run

by Saumil Shah – he had an interesting buffer overflow for the Linked-In client."

The EIP is the Instruction Pointer for the x86 architecture. The

purpose

of the EIP is to point to the next instruction in a particular

code segment.

If the EIP can be overwritten then the flow of control of an application can

be changed. In most cases this can lead to the execution of arbitrary code

on the targeted system. Hackers use this to penetrate vulnerable

systems.

–) Can you define a format string exploit?

"\* A format string exploit leverages what is considered a programming bug. If input is not sanitized, an attacker can perform calls to the stack; read, write, etc without knowing details about the EIP." Unfortunately this answer isn't accurate or detailed enough as almost all software vulnerabilities are the result of user input that is not properly sanitized or validated. A format string condition occurs when a user inserts a format token into a C based application and that input is not properly sanitized. Hence why it is called a format string vulnerability.

When that input hits a function that performs formatting, such as printf() the input is interpreted in accordance with the format tokens. Sometimes this can be used to write arbitrary data to arbitrary memory locations. The

EIP isn't

the only valuable memory location.

If you've managed to get this far, then you've survived reading

Michael's

answers to our questions. We're not going to spend much more

time writing

this review because by now we've formed our opinion. We did take

a quick

look at the PlanNetGroup's website and as with their people, we

were not the

least bit impressed.

Our opinion of the PlanNetGroup is that they'd have a hard time

hacking

their way out of a wet paper bag. Their security expert is not an expert by

our standards, as he did not properly answer any of our questions or help to

define any of their services. We're pretty sure that the PlanNetGroup could

run nessus and offer basic vulnerability assessment services.

We're also

pretty sure that they could offer IT services at some level. But

Re: [Full-disclosure] [Professional IT Security Providers –Exposed] PlanNetGroup ( F )

we'd hardly

call them subject matter experts and wouldn't recommend  
their

services to

anyone.

If you are using the PlanNetGroup services and feel that we  
have

not given

them a fair review then please comment on this post. We will

consider your

comments. We have to say that Jim and Michael were both  
very

polite,

friendly, and respectful, but we can't let their kind nature

impact our

opinion of their service delivery capabilities. We think that

they should

sit down and try to define their services properly. We also

think that they

should hire an ethical hacker with real world experience if  
they

intend to

protect anyone.

Score Card (Click to Enlarge)

[http://bp2.blogger.com/\\_VcwqM25xL9M/R5PxN8GqVTI/AAAAAAAAACU/D7T4RSQISXs/s1600-h/96YV5X.jpeg](http://bp2.blogger.com/_VcwqM25xL9M/R5PxN8GqVTI/AAAAAAAAACU/D7T4RSQISXs/s1600-h/96YV5X.jpeg)

Re: [Full-disclosure] [Professional IT Security Providers –Exposed] PlanNetGroup ( F )

—  
Posted By secreview to Professional IT Security Providers –

Exposed<<http://secreview.blogspot.com/2008/01/plannetgroup-f.html>>at 1/20/2008 04:21:00 PM

---

Full-Disclosure – We believe in it.  
Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>  
Hosted and sponsored by Secunia – <http://secunia.com/>

Regards,  
The Secreview Team  
<http://secreview.blogspot.com>

—  
Love Graphic Design? Find a school near you. Click Now.  
<http://tagline.hushmail.com/fc/Ioyw6h4fQlBYaiWpFnhi7pOK25eSsGhZHGXMnUnkrTsYbFDu13WWSE/>  
Professional IT Security Service Providers – Exposed

---

Full-Disclosure – We believe in it.  
Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>  
Hosted and sponsored by Secunia – <http://secunia.com/>

---

Full-Disclosure – We believe in it.  
Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>  
Hosted and sponsored by Secunia – <http://secunia.com/>