# Anonymous speaks: the inside story of the HBGary hack

By Peter Bright | Published 7 months ago

## A little help from my friends

Contained within Greg's mail were two bits of useful information. One: the root password to the machine running Greg's rootkit.com site was either "88j4bb3rw0cky88" or "88Scr3am3r88". Two: Jussi Jaakonaho, "Chief Security Specialist" at Nokia, had root access. Vandalizing the website stored on the machine was now within reach.

The attackers just needed a little bit more information: they needed a regular, non-root user account to log in with, because as a standard security procedure, direct ssh access with the root account is disabled. Armed with the two pieces of knowledge above, and with Greg's e-mail account in their control, the social engineers set about their task. The e-mail correspondence tells the whole story:

```
From: Greg
To: Jussi
Subject: need to ssh into rootkit
im in europe and need to ssh into the server. can you drop open up
firewall and allow ssh through port 59022 or something vague?
and is our root password still 88j4bb3rw0cky88 or did we change to
88Scr3am3r88 ?
thanks

-----------------------------------

From: Jussi
To: Greg
Subject: Re: need to ssh into rootkit
hi, do you have public ip? or should i just drop fw?
and it is w0cky - tho no remote root access allowed

-----------------------------------

From: Greg
To: Jussi
Subject: Re: need to ssh into rootkit
no i dont have the public ip with me at the moment because im ready
for a small meeting and im in a rush.
if anything just reset my password to changeme123 and give me public
ip and ill ssh in and reset my pw.

-----------------------------------

From: Jussi
To: Greg
Subject: Re: need to ssh into rootkit
ok,
it should now accept from anywhere to 47152 as ssh. i am doing
testing so that it works for sure.
your password is changeme123

i am online so just shoot me if you need something.

in europe, but not in finland? :-)

_jussi

-----------------------------------
```

```
From: Greg
To: Jussi
Subject: Re: need to ssh into rootkit
if i can squeeze out time maybe we can catch up.. ill be in germany
for a little bit.

anyway I can't ssh into rootkit. you sure the ips still
65.74.181.141?

thanks

---------------------------------

From: Jussi
To: Greg
Subject: Re: need to ssh into rootkit
does it work now?

---------------------------------

From: Greg
To: Jussi
Subject: Re: need to ssh into rootkit
yes jussi thanks

did you reset the user greg or?

---------------------------------

From: Jussi
To: Greg
Subject: Re: need to ssh into rootkit
nope. your account is named as hoglund

---------------------------------

From: Greg
To: Jussi
Subject: Re: need to ssh into rootkit
yup im logged in thanks ill email you in a few, im backed up

thanks
```

Thanks indeed. To be fair to Jussi, the fake Greg appeared to know the root password and, well, the e-mails were coming from Greg's own e-mail address. But over the course of a few e-mails it was clear that "Greg" had forgotten both his username *and* his password. And Jussi handed them to him on a platter.

Later on, Jussi did appear to notice something was up:

```
From: Jussi
To: Greg
Subject: Re: need to ssh into rootkit
did you open something running on high port?
```

As with the HBGary machine, this could have been avoided if keys had been used instead of passwords. But they weren't. Rootkit.com was now compromised.

## Standard practice

Once the username and password were known, defacing the site was easy. Log in as Greg, switch to root, and deface away! The attackers went one better than this, however: they dumped the user database for rootkit.com, listing the e-mail addresses and password hashes for everyone who'd ever registered on the site. And, as with the hbgaryfederal.com CMS system, the passwords were hashed with a single naive use of MD5, meaning that once again they were susceptible to rainbow table-based password cracking. So the crackable passwords were cracked, too.

So what do we have in total? A Web application with SQL injection flaws and insecure passwords. Passwords that were badly chosen. Passwords that were reused. Servers that allowed password-based authentication. Systems that weren't patched. And an astonishing willingness to hand out credentials over e-mail, even when the person being asked for them should have realized something was up.

The thing is, none of this is unusual. Quite the opposite. The Anonymous hack was not exceptional: the hackers used standard, widely known techniques to break into systems, find as much information as possible, and use that information to compromise further systems. They didn't have to, for example, use any non-public vulnerabilities or perform any carefully targeted social engineering. And because of their desire to cause significant public disruption, they did not have to go to any great lengths to hide their activity.

Nonetheless, their attack was highly effective, and it was well-executed. The desire was to cause trouble for HBGary, and that they did. Especially in the social engineering attack against Jussi, they used the right information in the right way to seem credible.

Most frustrating for HBGary must be the knowledge that they know what they did wrong, and they were perfectly aware of best practices; they just didn't actually *use them*. Everybody *knows* you don't use easy-to-crack passwords, but some employees did. Everybody *knows* you don't re-use passwords, but some of them did. Everybody *knows* that you should patch servers to keep them free of known security flaws, but they didn't.

And HBGary isn't alone. Analysis of the passwords leaked from rootkit.com and Gawker shows that password re-use is extremely widespread, with something like 30 percent of users re-using their passwords. HBGary won't be the last site to suffer from SQL injection, either, and people will continue to use password authentication for secure systems because it's so much more convenient than key-based authentication.

So there are clearly two lessons to be learned here. The first is that the standard advice is good advice. If all best practices had been followed then none of this would have happened. Even if the SQL injection error was still present, it wouldn't have caused the cascade of failures that followed.

The second lesson, however, is that the standard advice isn't good enough. Even recognized security experts who should know better won't follow it. What hope does that leave for the rest of us?