“WHAT IS THE ROOT USER?” JOSHUA SCHULTE SET UP THE SHARED “ROOT” PASSWORD HE’LL USE IN HIS DEFENSE

In a full day of testimony yesterday, one of Joshua Schulte’s former colleagues, testifying under the name Jeremy Weber (which may be a pseudonym of a pseudonym under the protective order imposed for the trial) introduced a ton of detail about how the engineering group he and Schulte worked in was set up bureaucratically, how the servers were set up, and how relations between Schulte and the rest of the group started to go south in the months and weeks leading up to the date when, the government alleges, he stole CIA’s hacking tools. He also described how devastating the leak was for the CIA.

In that testimony, the government began to lay out their theory of the case: When Schulte lost SysAdmin access to the servers hosting the malware they were working on — and the same day the unit announced they’d soon be moving the last server to which Schulte had administrator privileges under the official SysAdmin group — Schulte went back to the back-up file of the server from the day the fight started blowing up, March 3, 2016, and made a copy of it.

But the government also started previewing what will likely be Schulte’s defense: that some of these servers were available via a shared root password accessible to anyone in their group.

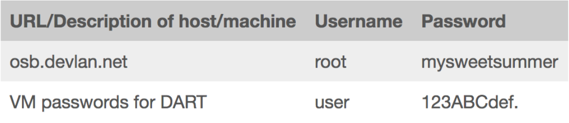
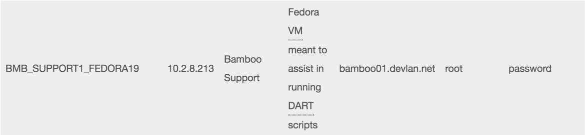
Prosecutor Matthew LaRoche walked Weber through a description of how a “root” user for the ESXi server was used.

> Q. What is the root user?

> A. The root user, in this situation, "root" was kind of Linux term for the administrative account on the machine, like the default administrator account.
>
> Q. You also mentioned there was a password for the ESXi server?
>
> A. That's correct.
>
> Q. Was that password stored anywhere?
>
> A. Yes, it was.
>
> Q. Where?
>
> A. It was stored on OSB's passwords page for some of our services.
>
> Q. What do you mean by OSB's passwords page?
>
> A. OSB had a lot of virtual machines outside of the Atlassian products that had passwords on them solely because the technology required to have a password and not for security practices, so that – these were often like test machines, and these passwords we kept on a page so that if somebody was leveraging that VM they would have the credentials they needed to log in to it.
>
> Q. Where was that passwords page located?
>
> A. Confluence.
>
> Q. Was it restricted in any way?
>
> A. It was.
>
> Q. How?
>
> A. It was to OSB.

This detail has been public since WikiLeaks first published the documents. I pointed it out here:

> Among the pages that got exposed in this week's Wikileaks dumps of CIA's hacking

> tools was a page of Operational Support Branch passwords. For some time the page showed the root password for the network they used for development purposes.
>
> 
>
> | URL/Description of host/machine | Username | Password |
> |---|---|---|
> | osb.devlan.net | root | mysweetsummer |
> | VM passwords for DART | user | 123ABCdef. |
>
> These passwords, as well as one (“password”) for another part of their server, were available on the network site as well.
>
> 
>
> | | | | | | | |
> |---|---|---|---|---|---|---|
> | BMB_SUPPORT1_FEDORA19 | 10.2.8.213 | Bamboo Support | Fedora VM meant to assist in running DART scripts | bamboo01.devlan.net | root | password |
>
> Throughout the period of updates, it included a meme joking about setting your password to Incorrect.
>
>
>

I CHANGED ALL MY PASSWORDS TO "INCORRECT".
> SO WHENEVER I FORGET, IT WILL TELL ME "YOUR PASSWORD IS INCORRECT."
>
> [snip]
>
> A discussion ensued about what a bad security practice this was.
>
>> 2015-01-30 14:30 [User #14588054]:
>>
>> Am I the only one who looked at this page and thought, “I wonder if security would have a heart attack if they saw this.”?
>>
>> 2015-01-30 14:50 [User #7995631]:
>>
>> Its locked down to the OSB group… idk if that helps.

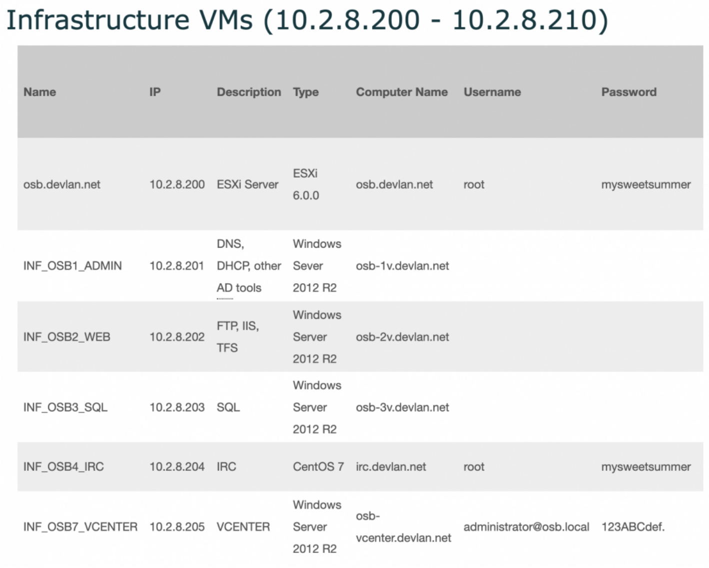
> > 2015-01-30 15:10 [User #14588054]:
> >
> > I noticed, but I still cringed when I first saw the page.
>
> I have no idea whether these passwords exacerbated CIA's exposure. The early 2015 discussion happened well before — at least as we currently understand it — the compromise that led to Wikileaks' obtaining the files.

It turns out that Schulte himself moved this password onto the ESXi passwords page on or before March 31, 2015, almost a year before he allegedly stole the files.

> MR. LAROCHE: Ms. Hurst, can you please publish Government Exhibit 1003, and please just zoom in on the top of the email, the to-from.
>
> Q. Is this another email from the CIA, Mr. Weber?
>
> A. Yes, it is.
>
> Q. When was this email sent?
>
> A. It was sent on March 31, 2015, at 8:20 p.m.
>
> Q. Who sent it?
>
> A. It was sent by Josh Schulte.
>
> Q. Who was it sent to?
>
> A. It was sent to the OSB email group.
>
> Q. How do you know that?
>
> A. The string NCS-IOC-EDG-AED-OSB is a user group and it's explicit in its naming. NCS was in the org chart above IOC, the rest of those are the groups that we have previously talked about.
>
> Q. It's a lot of acronyms.
>
> A. It is.

> Q. Below that, what’s the subject line?
>
> A. OSB.DevLAN.net VM credentials.
>
> Q. What’s OSB.DevLAN.net?
>
> A. That was the OSB ESXi server.
>
> MR. LAROCHE: Ms. Hurst, if you could please zoom out and then on to the text of the email.
>
> Q. Can you read the first sentence, please?
>
> A. “I’ve modified the OSB’s ESXi server page to contain the passwords and other information directly instead of through the OSB’s passwords page; also updated the permissions to be restricted to everyone outside of OSB.”
>
> Q. Do you understand what he’s referring to by OSB’s ESXi server page?
>
> A. Yes.
>
> Q. What’s he referring to?
>
> A. It was a second page created later to contain information specifically to the ESXi server and the administration of that.
>
> Q. And do you understand what he means by updated the permissions to be restricted to everyone outside of OSB?
>
> A. This was him saying that only people within the OSB — within OSB would have access to read this page.
>
> Q. Now, is this the same ESXi server that as of 2015 was running Confluence and Bamboo?
>
> A. Yes, it was.

I think this is what that page would have looked like, in part, in the March 3, 2016 files, with the same root password set to “mysweetsummer:”



Infrastructure VMs (10.2.8.200 - 10.2.8.210)

Name	IP	Description	Type	Computer Name	Username	Password
osb.devlan.net	10.2.8.200	ESXi Server	ESXi 6.0.0	osb.devlan.net	root	mysweetsummer
INF_OSB1_ADMIN	10.2.8.201	DNS, DHCP, other AD tools	Windows Sever 2012 R2	osb-1v.devlan.net		
INF_OSB2_WEB	10.2.8.202	FTP, IIS, TFS	Windows Server 2012 R2	osb-2v.devlan.net		
INF_OSB3_SQL	10.2.8.203	SQL	Windows Server 2012 R2	osb-3v.devlan.net		
INF_OSB4_IRC	10.2.8.204	IRC	CentOS 7	irc.devlan.net	root	mysweetsummer
INF_OSB7_VCENTER	10.2.8.205	VCENTER	Windows Server 2012 R2	osb-vcenter.devlan.net	administrator@osb.local	123ABCdef.

Schulte will eventually argue that he not only recognized that this arrangement — which he set up, per this email — was insecure, but that he warned people about it repeatedly. Weber says that didn’t happen, because if Schulte had complained, he would have told Schulte to fix it.

> Q. Are you sure that the defendant never made any complaints that DevLAN was vulnerable to theft?
>
> A. Yes.
>
> Q. Why?
>
> MS. SHROFF: Objection.
>
> THE COURT: Overruled.
>
> A. If he had complained to me about the Atlassian products being vulnerable to theft, I would have told him to fix it. The Atlassian products were our responsibility, and if he had highlighted an issue with that, I would have made it our primary focus to fix that.

The government has already begun showing forensics suggesting the files were stolen via other means.

More importantly, they showed that if Schulte thought the shared root password was insecure, he’s got no one but himself to blame for it.

It’s certainly possible he will point to things he’ll argue are proof that he raised concerns about this arrangement — rather than just joking about it on the development pages (it won’t take too long before we learn which numbered ID WikiLeaks used for Schulte). But there’s already evidence that he’s the one who set it up that way.

Calyx Institute has generously sprung for Schulte transcripts. If you’d like to support the effort, you can make a tax deductible donation to them here.