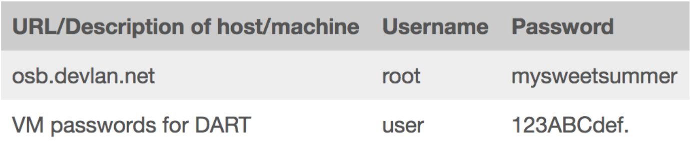
PASSWORD: 0SBP@SS

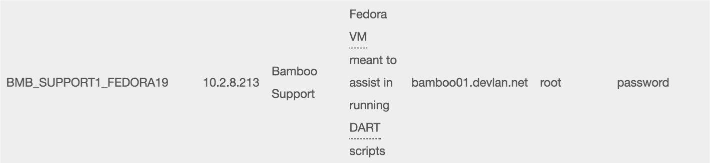
Remember how infosec people made fun of John Podesta when they learned his iCloud password — which got exposed in the Wikileaks dump of his stolen emails — was Runner4567? 4Chan used the password to hack a bunch of Podesta's accounts.

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."

At the beginning of January 2015, it included the passwords for two unclassified laptops used by the department, one of which was the very guessable 0sbP@ass.

> OSB unclass laptop #1 password (tag 2005K676, Dell service tag: 7731Y32): “OSBDemoLap9W53!” (Without quotes)
>
> OSB unclass laptop #2 password (tag 2005K677, Dell service tag: CN81Y32): “0sbP@ss” (no quotes, first chracter is a zero)

Remember, Assange has claimed that CIA treated its exploits as unclassified so they could be spread outside of CIA facilities.

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. The laptops themselves were unclassified, and would only be a problem if someone got physical custody of them. Though shared devices like laptops were one of the things for which CIA had a multi-factor authentication problem up until at least August of 2016.

But if we’re going to make fun of John Podesta for password hygiene exposed in a Wikileaks dump, we ought to at least acknowledge that CIA’s hackers, people who spent their days exploiting hygiene sloppiness like this, had (simple) passwords lying around on a server that — as it turns out — was nowhere near as secure as it needed to be.