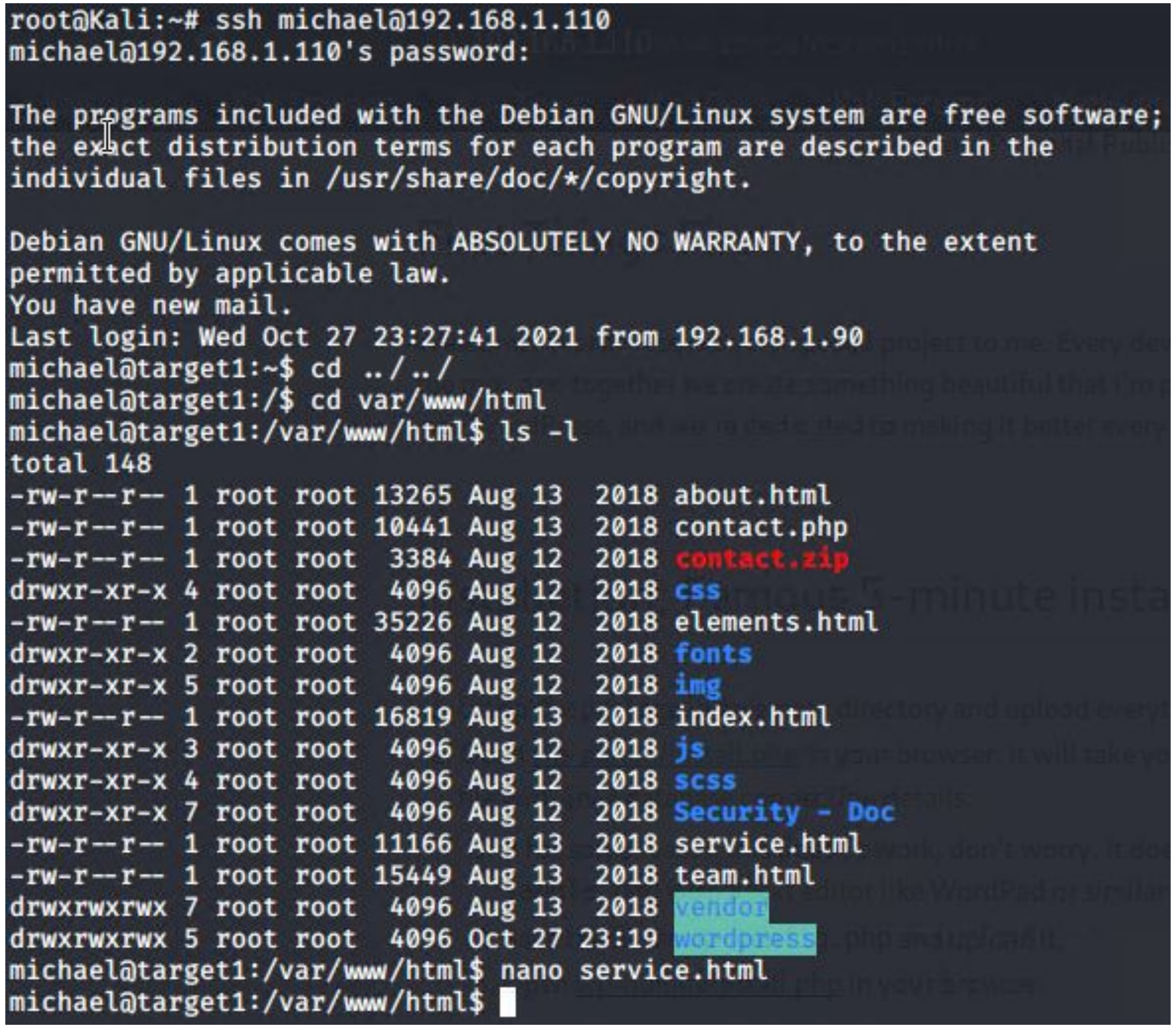
Stealth Exploitation of Open Port 22 SSH and Weak Passwords

Monitoring Overview

- SSH Login Alert would detect this exploit
- Monitor SSH Port for unauthorized access
- Triggers when user attempts to access system over Port 22

Mitigating Detection

- SSH through a different open port that is less obvious
- Other exploit ideas: reverse shell exploit



```
root@Kali:~# ssh michael@192.168.1.110
michael@192.168.1.110's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Wed Oct 27 23:27:41 2021 from 192.168.1.90
michael@target1:~$ cd ../../
michael@target1:/$ cd var/www/html
michael@target1:/var/www/html$ ls -l
total 148
-rw-r--r-- 1 root root 13265 Aug 13  2018 about.html
-rw-r--r-- 1 root root 10441 Aug 13  2018 contact.php
-rw-r--r-- 1 root root  3384 Aug 12  2018 contact.zip
drwxr-xr-x 4 root root  4096 Aug 12  2018 css
-rw-r--r-- 1 root root 35226 Aug 12  2018 elements.html
drwxr-xr-x 2 root root  4096 Aug 12  2018 fonts
drwxr-xr-x 5 root root  4096 Aug 12  2018 img
-rw-r--r-- 1 root root 16819 Aug 13  2018 index.html
drwxr-xr-x 3 root root  4096 Aug 12  2018 js
drwxr-xr-x 4 root root  4096 Aug 12  2018 scss
drwxr-xr-x 7 root root  4096 Aug 12  2018 Security - Doc
-rw-r--r-- 1 root root 11166 Aug 13  2018 service.html
-rw-r--r-- 1 root root 15449 Aug 13  2018 team.html
drwxrwxrwx 7 root root  4096 Aug 13  2018 vendor
drwxrwxrwx 5 root root  4096 Oct 27 23:19 wordpress
michael@target1:/var/www/html$ nano service.html
michael@target1:/var/www/html$ 
```