

Security Assessment of: HP-Pavilion-15-Notebook-PC

Owner: Eoin Dalton

Operating System: Ubuntu 18.04 LTS

Processor Type: Intel® Core™ i3-5010U CPU @ 2.10GHz × 4

Graphics: Intel® HD Graphics 5500 (Broadwell GT2)

OS Type: 64bit

Disk: 2.0 TB

Contents

High Level Assessment	2
What needs to be protected?	2
Who owns it?	2
Who needs to access it?	2
Where is the information stored?	2
What would the impact of a breach be?	2
Examine Specific Threats and Countermeasures	3
Protection against malicious software - viruses, spyware, etc.?	3
Firewall?	3
Open Ports	4
Wireshark Capture	5
OS and Software	5
Accounts and Passwords	5
Browser Settings	6
References	7
Figure 1: Firewall	3
Figure 2: IPtables	3
Figure 3: Open ports	4
Figure 4: Wireshark Capture	5
Figure 5: OS Software Update	5
Figure 6: Lastpass	6
Figure 7: Browser Preferences	6

High Level Assessment

What needs to be protected?

The physical computer needs to be protected at home as I have to small children that would love to touch and possibly break it this would lead to serious down time for collage work at home. The hardware needs to be protected as it can be breached if someone has a USB they can boot another operating system and view the hard disk. The data need to be protected as some is sensitive such as collage documents.

Who owns it?

This is my own personal computer.

Who needs to access it?

As this is a personal computer the only access needed is by me and my wife.

Where is the information stored?

The information is stored in my one-drive folder that is synchronized to my Microsoft account in the cloud. There is also a Dropbox folder which is my backup account and all-important documents are backed up to this account in the cloud. There are some less important files stored in my documents folder on the desktop.

What would the impact of a breach be?

If this machine was breached the attacker can gain access to personal files stored on the computer. By using the browser, they may be able to brute force my Lastpass account to gain access to my account and passwords. Possibly I would have to closing accounts that were affected. If it was infected by malicious software or stolen I would face the prospect of down time for collage work as it would take time to clean or to buy a new laptop as I would need to re-install all applications.

Examine Specific Threats and Countermeasures

Protection against malicious software - viruses, spyware, etc.?

Currently there is no anti-virus software installed. I am new to Linux, so I am learning the best practices for protecting my PC. I have reviewed the Ubuntu website and the advice is that there are not many viruses that affect Linux, so the view is there is no need for anti-virus software.

Firewall?

If you look at the screen shot below you can see that my firewall is inactive. Ubuntu comes with a firewall built in.

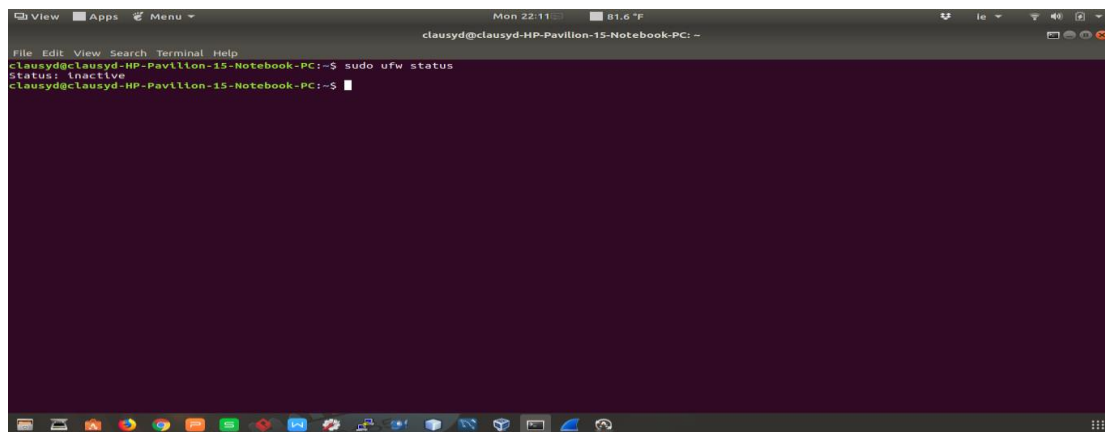


Figure 1: Firewall

It uses Iptables where I can restrict IP ranges or protocols. See screen shot below. Now I have no configurations done, but according to (Help.ubuntu.com, 2018) all traffic is allowed by default.

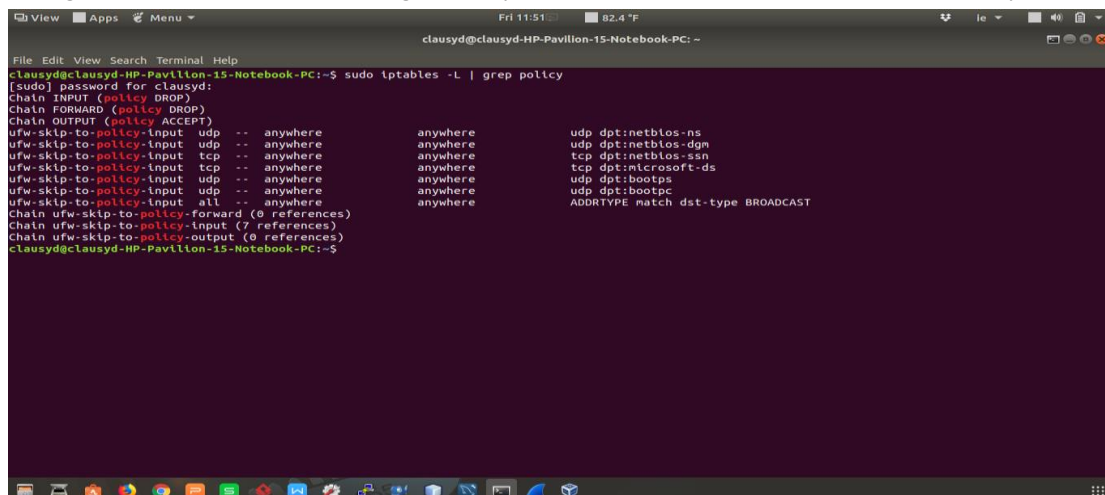
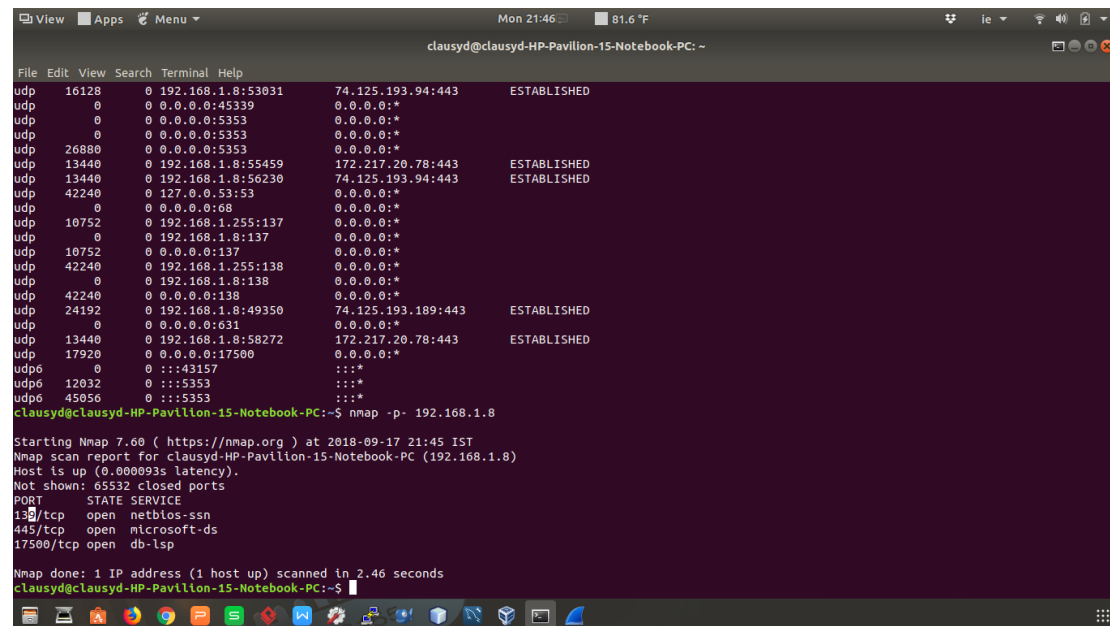


Figure 2: Iptables

Open Ports

After running a command on Ubuntu, I can check all open ports on the machine. Please see screen shot below for more details.



```

File Edit View Search Terminal Help
udp 16128 0 192.168.1.8:53031 74.125.193.94:443 ESTABLISHED
udp 0 0 0.0.0.0:45339 0.0.0.0:*
udp 0 0 0.0.0.0:5353 0.0.0.0:*
udp 0 0 0.0.0.0:5353 0.0.0.0:*
udp 26880 0 0.0.0.0:5353 0.0.0.0:*
udp 13440 0 192.168.1.8:55459 172.217.20.78:443 ESTABLISHED
udp 13440 0 192.168.1.8:56230 74.125.193.94:443 ESTABLISHED
udp 42240 0 127.0.0.53:53 0.0.0.0:*
udp 0 0 0.0.0.0:68 0.0.0.0:*
udp 10752 0 192.168.1.255:137 0.0.0.0:*
udp 0 0 192.168.1.8:137 0.0.0.0:*
udp 10752 0 0.0.0.0:137 0.0.0.0:*
udp 42240 0 192.168.1.255:138 0.0.0.0:*
udp 0 0 192.168.1.8:138 0.0.0.0:*
udp 42240 0 0.0.0.0:138 0.0.0.0:*
udp 24192 0 192.168.1.8:49350 74.125.193.189:443 ESTABLISHED
udp 0 0 0.0.0.0:631 0.0.0.0:*
udp 13440 0 192.168.1.8:58272 172.217.20.78:443 ESTABLISHED
udp 17920 0 0.0.0.0:17500 0.0.0.0:*
udp6 0 0 :::43157 :::*
udp6 12032 0 :::5353 :::*
udp6 45056 0 :::5353 :::*
clausyd@clausyd-HP-Pavilion-15-Notebook-PC:~$ nmap -p- 192.168.1.8

Starting Nmap 7.60 ( https://nmap.org ) at 2018-09-17 21:45 IST
Nmap scan report for clausyd-HP-Pavilion-15-Notebook-PC (192.168.1.8)
Host is up (0.000093s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
17500/tcp open  db-lsp
Nmap done: 1 IP address (1 host up) scanned in 2.46 seconds
clausyd@clausyd-HP-Pavilion-15-Notebook-PC:~$

```

Figure 3: Open ports

As you can see from the screen shot I have three open ports. After a quick Google search I can see that 17500 is a port that Dropbox synchronizes on which make sense because I have Drobox link with the computer. Port 139 is NetBIOS setting. According to (SpeedGuide, 2018) this port has some vulnerabilities and it say “By default, when File and Print Sharing is enabled it binds to everything, including TCP/IP (The Internet Protocol), rather than just the local network, meaning your shared resources are available over the entire Internet for reading and deletion, unless configured properly. Any machine with NetBIOS enabled and not configured properly should be considered at risk” (SpeedGuide, 2018). The last port open is 445 is used for direct TCP/IP MS Networking access without the need for a NetBIOS layer.

Wireshark Capture

Wireshark capture of browsing activity over wlo1. I done a capture of me logging onto Moodle. Wit with user name and password and all the packets look to be encrypted. See screen shot below. If the website was not encrypted I would be able to see my user name and password on Wireshark here. To the left I can see hex decimal values and Wireshark tries to show this in plain text on the right. In my browser setting I have SSL connection enabled so all packet should be encrypted.

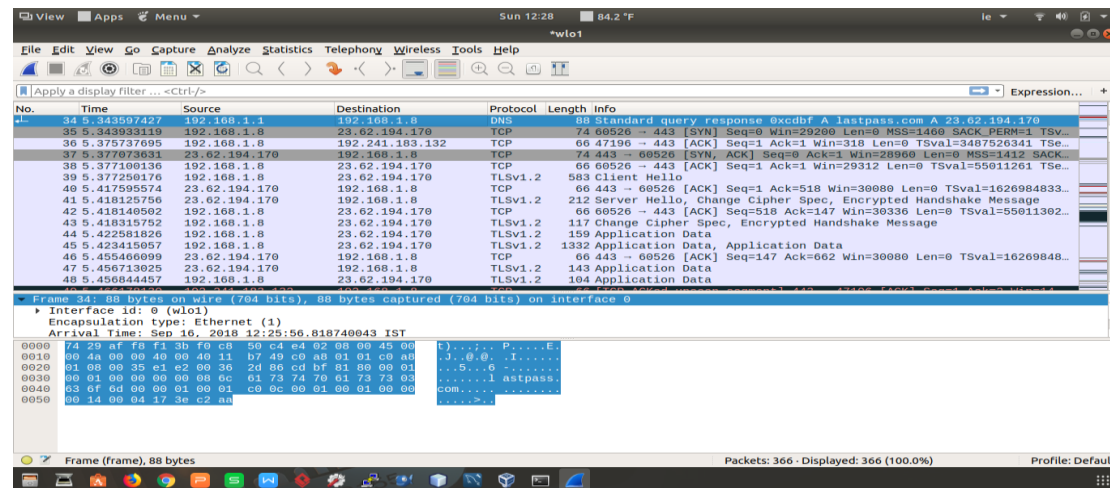


Figure 4: Wireshark Capture

OS and Software

All software updates are installed. I would do an update weekly.

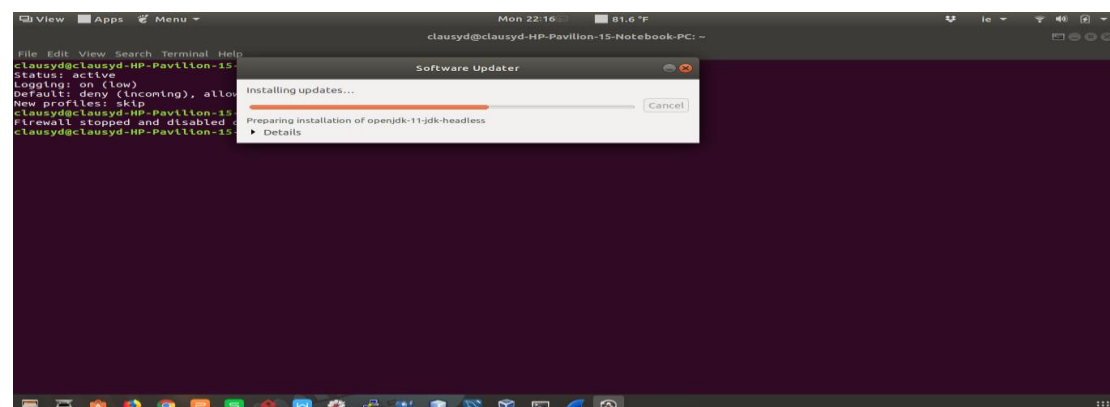


Figure 5: OS Software Update

My OS has a password to protect it, but if a person got hold of my computer they could possibly compromise it by booting from a USB or live cd they can then get access to my hard disk.

Accounts and Passwords

Up until last month I google stored all my passwords, now I am using Lastpass to store all accounts usernames and passwords. Lastpass uses a master password to logon and I have

multi-factor authentication set with Google authentication. Lastpass can launch sites and log me in automatically.

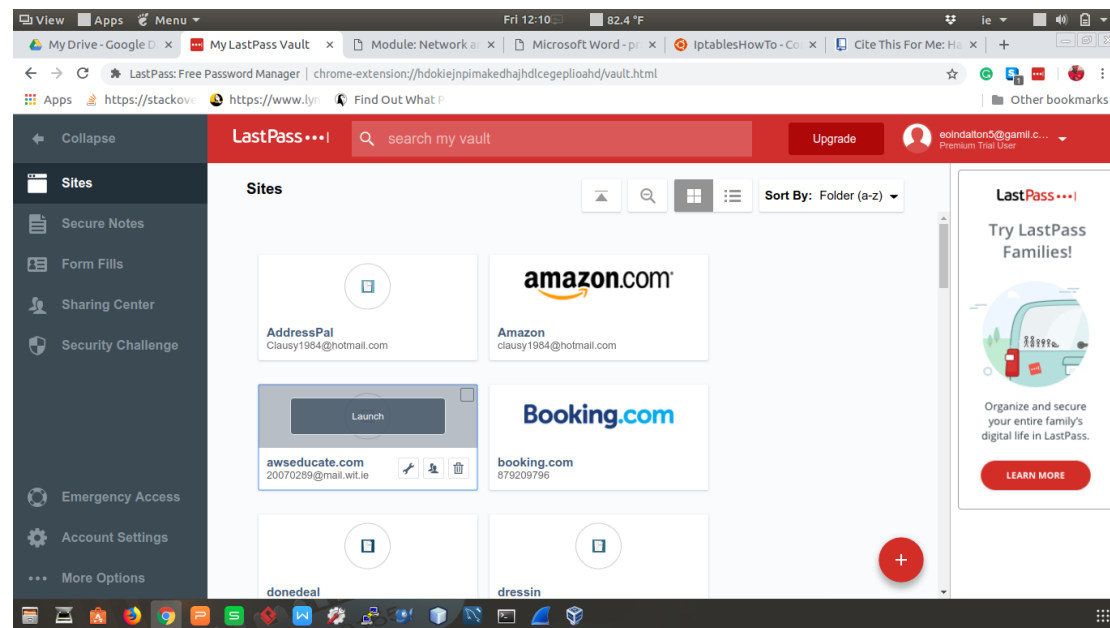


Figure 6: Lastpass

Browser Settings

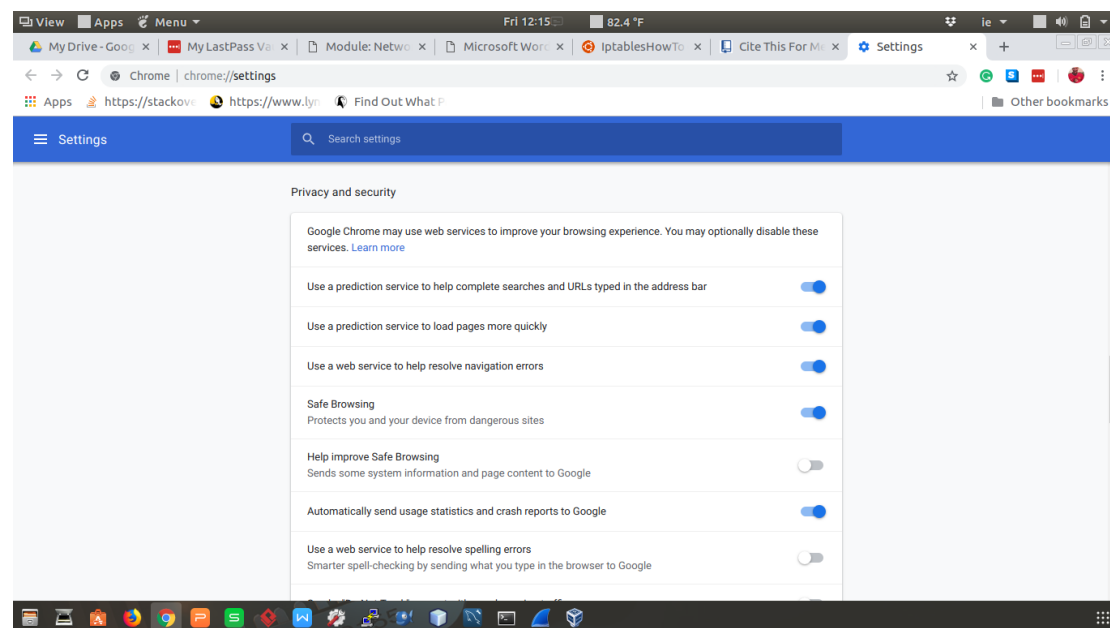


Figure 7: Browser Preferences

I am using Google Chrome for my browser; above is a screenshot you can see I have saved browsing activated. Safe browsing shows me notification when I visit a dangerous website, or I am about to download a malicious file. I have HTTPS everywhere activated. This is an extension

for Firefox and Chrome. This will use SSL to encrypt all my traffic, “Sadly, many sites still include a lot of content from third party domains that is not available over HTTPS. As always, if the browser's lock icon is broken or carries an exclamation mark, you may remain vulnerable to some adversaries that use active attacks or traffic analysis “(Electronic Frontier Foundation, 2018).

References

Electronic Frontier Foundation. (2018). HTTPS Everywhere. [online] Available at: <https://www.eff.org/https-everywhere> [Accessed 21 Sep. 2018].

Help.ubuntu.com. (2018). IptablesHowTo - Community Help Wiki. [online] Available at: <https://help.ubuntu.com/community/IptablesHowTo> [Accessed 21 Sep. 2018].

SpeedGuide. (2018). Port 139 (tcp/udp). [online] Available at: <https://www.speedguide.net/port.php?port=139> [Accessed 17 Sep. 2018].