Answers

GDPR – It is a regulation in the EU on data protection and privacy within the EU (European Union) and EEA (European Economic Area)

Hannah’s Broken Hard Drive – First it didn’t show up, so we changed the cord (Physical). Then view it in the explorer but disappeared or crashed. After tried formatting using the default fix, but that failed. Also partitioning format failed. Running check disk didn’t work and had to turn off read only to have it not be able to read anything from explorer anymore. I was going to do Gparted but didn’t show up, so Matthews dad ran a scan on it. There was a numerous number of bad sectors on it so that is why it couldn’t read it. The MBR (Master boot record) was still in tack but damaged and that is why we could see the RAW format of the drive but couldn’t do anything with it.

Ctfmon.exe – Also Known as CTF Loader, is involved with the alternative language input services. This will be in runup as long as there is a need for Text services and speech applets. IS NOT REQUIRED BUT SUGGESTED. MOST KNOWN For software’s creating one named the same one but a trojan horse.

FCRA (Fair Credit Reporting Act) – Legislation enacted to promote the accuracy, fairness and privacy of consumer information. It was enacted in 1970 and enforced by the US Federal Trade Commission, Consumer Financial Protection Bureau, and private litigants.

David Network Error on laptop – The problem was that David was getting a network error ERR\_AUTHENTICATE\_ERROR. This lead to the problem of he could not access some websites one of those being YouTube for some reason. That didn’t stop it from accessing other websites though. The solution that I found was you had to reset the proxy on the computer. This fixed it because I later figured out that the problem was the computer couldn’t reach some files because of the proxy.

Kali USB Shutting down and loading problems – When we had a problem wit the usb shutting down or loading up the error was most likely that the ISO was incorecctly placed on the USB, that the USB is becoming corrupted or has already been corrupted.

Creating persistence on USB with Kali – There is a software that is called partition wizard that we were able to create a 8 gb partition then put the Kali on one of those. It worked better than trying to parititon once you got kali to boot up.

USB missing a driver – So we started out by uninstalling the driver and that is only if it does come up. It sometimes comes up in linux but not in Windows. This is because of corruption of the USB. For some usb there is a program that can clear the Rom on a USB and Hyundai. For that specific usb that was not the case.

JC Brother Surface PC – There was an error that wouldn’t let you do anything with the hard drive. You couldn’t at all make a file read a file or anything. You were able to load up into windows tho and there was a problem with external hard drive that didn’t even load on another windows 7 computer. Not sure but couldn’t see the computer so not 100% sure. Dad said it may be a crypto virus, ransomware or something like that.

Switch USB not working – So the dock USB started not to work or would work eventually after keeping it plugged in. The problem with that is pairing new controllers. We tested that it was the switch by switching out the docks but the same problem happened. I found the solution on a youtube video online that said remove the switch from the dock and completely shut it down. Wait about 10 – 15 seconds (I waited a minute). Then put it straight on the dock and it will turn on itself and that worked.

Burp not finding any host – The problem was when I started it out burp could find nothing. At that point I turned off the proxy and it couldn’t find the server. I found out that I needed to look into the /etc/resolvconf folder. I found in there that the run should be a directory but was a broken link. Rewritting it didn’t work but the following commands worked  
sudo apt-get purge resolvconf  
sudo apt-get install resolvconf  
sudo systemctl enable resolvconf (Autocorrected to resolvconf.service)  
[optional] sudo systemctl start resolvconf  
This is also useful in almost any cases that you get the error saying the server will not start. Also when you go and get the file, It says that it is broken.

Not being able to move windows files (Specifically the Windows.old folder). This became a problem and was given the error “ACCESS DENIED”. I looked it up and to fix this I took control of those files using   
takeown /F "C:\Windows.old" /R /D Y  
After I had to speed up the transferring because it was 30 GB and read that Robocopy was faster. I later figured out that it was also capable of doing multithreading so I copied all the files to hard drive using  
robocopy /MOVE /E "C:\Windows.old" E:\Windows.old\Predator\Windows.old /mt:128

The BlueBorne computer virus was discover by Armis. The virus is an airborne virus because it travels via Bluetooth. The best [article](https://www.armis.com/blueborne/) on it explains that this was a huge attack as it effects every device that has Bluetooth. Not only that but completely takes over and gives unlimited access to hacker.

What happens when there are 2 devices with the same mac address – First of all if they don’t talk to each other or aren’t on the same network than it doesn’t matter. If they happen to be and the table has both of them in it then they don’t send any packets to either device. Simple and smart solution in my opinion.

Transposition Cipher genre – The transposition cipher includes multiple ciphers as it is just a definition. One example is rail fence cipher. You take the plain text and put it in a pattern using keys as the height and width of the pattern. Then you take that new format and read it like a normal human being and there is your cipher text.

Heart bleeding attack – This is an attack included in Metasploit that is fairly understandable based on reading [this website](https://null-byte.wonderhowto.com/how-to/hack-like-pro-hacking-heartbleed-vulnerability-0154708/). It gets its name as sending data you slowly get responses that give you more and information about that machine.

Error 15299 on the Pavilion Laptop – This laptop had a problem with the touch screen after a while. It wasn’t a hardware problem but a windows driver issue. This can be established by it worked on bootup diagnostics and in Linux but not windows. It happened and one solution was to uninstall the HID driver but that is temporary. It eventually just didn’t work.

How to break into GMC Canyon – There is this car that won’t move in the neighborhood and I was wondering if there was an easy way to break into it.The only way that is possible is breaking in to a car like you break into any other car. Nothing special and just a basic car.

The Eggshell application on Github – Notorious for being ran in kali this is a repository that can take control of an iPhone and control some parts of it. Based on this [website](https://www.hacking.land/2017/08/eggshell-iosmacos-remote-administration.html?m=1) it says that the device needs to be jailbroken but with the ip address you can get access to almost anything and upload/download information.

Emulating of an android – I looked up and it was a while ago with the best one being on this [website](https://www.how2pc.com/best-android-emulator-2018/). It was made a while back but the one I have notes on are the KO. Like the other ones I tried something that uses all the types of technology. It was Pokémon go and past the sign in it didn’t work because of the location and running the app was trouble. I gave up after this and figured out that all of them were like this and KO was the middle ground for all of them.

Good Repositories

* [Red Hawk](https://github.com/Tuhinshubhra/RED_HAWK) – Good for gathering information and vulnerability scanner
* [Lazy Script](https://github.com/arismelachroinos/lscript) – A script that commands to other programs
* [Awesome For Beginners](https://github.com/MunGell/awesome-for-beginners) – List of useful programs
* [Awesome CTF](https://github.com/apsdehal/awesome-ctf) – Names of software’s that could be useful in CTF contest
* [Nikto](https://tools.kali.org/information-gathering/nikto) – A vulnerability scanner built in Perl
* [Metadata Extractor](https://github.com/drewnoakes/metadata-extractor) – Extracts the Metadata of files (Shocking I know)
* [Awesome Hacking](https://github.com/Hack-with-Github/Awesome-Hacking) – List of useful repositories
* [Termineter](https://tools.kali.org/stress-testing/termineter) – For smart Meter Testing (Not sure what that means)

Practice Materials

* [Over the wire Wargames](https://overthewire.org/wargames/) – SSH into the challenge servers
* [Smash the Stack](http://smashthestack.org/wargames.html) – Wargames website
* [Hellbound Hackers](https://www.hellboundhackers.org/) - Every challenge under the sun (FAVORITE)
* [Metasploitable](https://sourceforge.net/projects/metasploitable/) – Vulnerable Linux VM
* [Defend the Web](https://defendtheweb.net/dashboard) – Great tutorial/starting place
* [Fedora](http://www.computersecuritystudent.com/UNIX/FEDORA/lesson1/index.html) – VM instructions
* [Resource List](https://captf.com/practice-ctf/) – List of so many website resources
* [Vulnhub](https://www.vulnhub.com/resources/) – Tutorial Resources page

Def con Presentation Requirements – The way to present is to submit the papers. It is not required to be in the field for a specific amount of time, but to come up with something to present.

Showing hard drive but not reading data – So the hard drive would come up when plugged in but the driver would sometimes have an issue coming up and sometimes it would not come up, but for the most part it would show up. 95% of the time it would not be able to open but sometimes it would open slowly and then not load any files. The reason for this is because it was dropped while powered on. Because of this the arm was reading and was broken. A suggested fix for this would be to change it to quick removal (NOT TESTED, not sure if will work)

Full College CIS class – On this [website](http://www.cs.fsu.edu/~redwood/OffensiveComputerSecurity/lectures.html) it they post the whole curriculum and all the videos for each week on it.

Python issue with pip – When it gave me a lot of red text it is because the path had a pip in it for another location. The issue is also that if it is in the Program Files (x86) folder you will have to run it in administration mode. Also I deleted the other script so there wasn’t an issue later on.

Pass the Hash (PtH) – a method of authenticating a user without knowing the users password (Cleartext)

Disabling Microsoft Edge to Run on Startup – So this was a little more complex than I wanted. The way that I got from this [website](https://www.windowscentral.com/how-prevent-loading-microsoft-edge-processes-startup-windows-10#:~:text=Search%20for%20gpedit.,the%20Local%20Group%20Policy%20Editor.&text=On%20the%20right%20side%2C%20double,Select%20the%20Disabled%20option.) was that it required an administrative tool known as Local group management. This was through gpedit.msc and then it tells you from there. The issue is my computer did not have that file so I had to get it downloaded. Below is how to download it through a short bat command

Installing Local Group Policy Editor – Put the below in a bat file and run it as admin.  
@echo off   
pushd "%~dp0"   
  
dir /b %SystemRoot%\servicing\Packages\Microsoft-Windows-GroupPolicy-ClientExtensions-Package~3\*.mum >List.txt   
dir /b %SystemRoot%\servicing\Packages\Microsoft-Windows-GroupPolicy-ClientTools-Package~3\*.mum >>List.txt   
  
for /f %%i in ('findstr /i . List.txt 2^>nul') do dism /online /norestart /add-package:"%SystemRoot%\servicing\Packages\%%i"   
pause

This should be able to install all of it correctly. If not you are just fucked.