Intro - What is DEFCON

DEFCON is one of the largest cybersecurity conventions in the world. Every year it takes place in Vegas and brings people from all over. Having all of those hackers in one place makes for a fun environment with lots of learning opportunities, but it also makes an environment where your threat model has to be a little bit more extreme.

Figure 1: DEFCON logo

My Threat Model

The bottom line is I am not a particularly interesting person to hack. I am a 16 year old without a bank account to speak of. This however does not mean I will not secure my things.

The main attackers I am protecting against are people who want to hack into laptops and phones for the sake of doing it. This means I am likely spared from any new zero days that could be better spent on world leaders.

One of the main motivators for securing my electronics is fun. I am going a little bit further than I probably need to.

Attack Vectors

My three biggest concerns are 1. Downloading malware (as always) 2. Getting my electronics stolen 3. Network/Wireless attacks

Downloading Malware

I think the general digital hygiene that I take in my day to day life is probably strong enough to protect against downloading malware. I only download signed packages from my package manager, and if I am downloading something that is not from my package manager I make an effort to read the source code.

I don't think my risk of downloading malware goes up significantly at DEF CON because I don't plan on downloading software at all.

Getting My Electronics Stolen

There is always a risk of getting electronics stolen, especially when you are traveling. This is not a DEF CON specific risk, but I think it is enough of a risk to be worth mentioning.

To mitigate the damage that could be caused by getting my electronics stolen I have both my laptop and phone full disk encrypted. I don't think my laptop is likely to be stolen because it is an old Thinkpad that I found in the trash, but I will keep an extra close eye on my phone.

Full disk encryption should make it so that the only damage that would come from getting my laptop or phone stolen, is that I would no longer have a laptop or phone. I would not have to worry about any saved logins or other sensitive information.

Wireless/Network Attacks

I am writing about this more because it is fun to mitigate these attacks, than because they are a tremendous risk to me. They are much more of a risk for people with more aggressive threat models.

Wall of Sheep

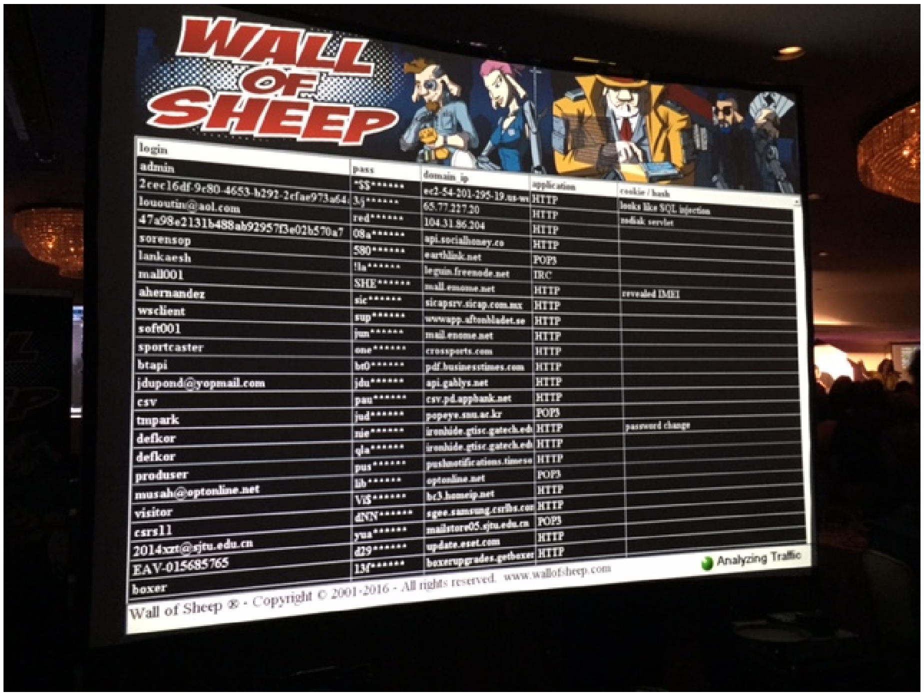
I believe the highest wireless attack risk for me is ending up on the wall of sheep. The wall of sheep is a list of the usernames and passwords of people who were not using proper encryption when they logged into something on the insecure DEF CON network.

I plan on staying off the wall of sheep by only connecting to the internet though a tethered hotspot. This should eliminate the risk because the wall of sheep only includes people from the insecure DEF CON network.

Overall Wireless Safety

I am going to turn off WiFi and bluetooth on both my laptop and phone, and only communicate with the outside world over LTE.

PDF Version

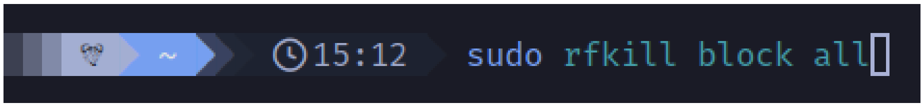


login	pass	domain ip	application	cookie / hash
admin	*$$******	ec2-54-201-295-19.us-we	HTTP	
2cee16df-9c80-4653-b292-2cfae973a64	3/j******	65.77.227.20	HTTP	looks like SQL injection
lououtin@aol.com	red******	104.31.86.204	HTTP	zodiak servlet
47a98e2131b488ab92957f3e02b570a7	08a******	api.socialhoney.co	HTTP	
sorensop	580******	earthlink.net	POP3	
lankaesh	!la******	leguin.freenode.net	IRC	
mall001	SHE******	mail.enome.net	HTTP	revealed IMEI
ahernandez	sic******	sicapsrv.sicap.com.mx	HTTP	
wsclient	sup******	wwwapp.aftonbladet.se	HTTP	
soft001	jun******	mail.enome.net	HTTP	
sportcaster	one******	crossports.com	HTTP	
btapi	bt0******	pdf.businesstimes.com	HTTP	
jdupond@yopmail.com	jdu******	api.gablys.net	HTTP	
csv	pau******	csv.pd.appbank.net	HTTP	
tmpark	jud******	popeye.snu.ac.kr	POP3	
defkor	nie******	ironhide.gtisc.gatech.edu	HTTP	password change
defkor	qla******	ironhide.gtisc.gatech.edu	HTTP	
produser	pus******	pushnotifications.timeso	HTTP	
musah@optonline.net	lib******	optonline.net	POP3	
visitor	ViS******	bc3.homeip.net	HTTP	
csrs11	dNN******	sgee.samsung.csrlbs.com	HTTP	
2014xxt@sjtu.edu.cn	yua******	mailstore05.sjtu.edu.cn	POP3	
EAV-015685765	d29******	update.eset.com	HTTP	
boxer	13f******	boxerupgrades.getboxer	HTTP	

Wall of Sheep ® - Copyright © 2001-2016 - All rights reserved. www.wallofsheep.com

Analyzing Traffic

Figure 2: Image of Wall of Sheep



```
sudo rfkill block all
```

Figure 3: Running rfkill Command