SHADØW SYND1CATE

Presents:

The Hacker Summer Camp Survival Guide

Authored By:
Collin Montenegro ("Unkn0wn")
🐦 @_Unkn0wn1
&
Alexander Delgado ("Byt3")
🐦 @0xalexdegado

Table of Contents

Introduction

With "Hacker Summer Camp" (i.e. DEF CON, BSidesLV, BlackHat, etc.) right around the corner, many members and other individuals have been asking the question, "How do you go about making the best out of all the conferences and events?". We know that with the increase in size, and what seems like endless things to attend and do, the conferences can be flat out intimidating. This is why we decided to put together this short E-book to help provide you with some insight and knowledge based on our previous experiences on how to tackle the famous week of "Hacker Summer Camp"!

This book is broken down into four distinct sections. In the first section we will cover how to properly setup and configure your cell phone to help keep it secure while at the conferences. This is followed up by a similar section except this time we discuss tips and guidance on how to properly configure your laptop. Next, we will dive into BSidesLV and give you background on what it is, what it offers, and provide some tips on how to tackle this Con! Lastly, we will jump into DEF CON outlining the same key points in order to help make the world's largest hacker conference not as daunting.

Something to keep in mind while reading this book, by no means are we insinuating that you take this as the gold standard. There is just far too much to fully cover every single minute point. To include, some people may even have differing thoughts or other suggestions to add! If you do have any recommendations on things we should add or even edit, please by all means reach out to us! This was created to help the community and we would love to make this a living document that we can continue to update each year.

In the end, we hope this book suits you well and makes your Hacker Summer Camp experience an amazing one that you won't want to forget!

- *Collin Montenegro*

- *Alexander Delgado*

Cell Phone Preparation Checklist & Tips

Preparation Checklist

☐ Backup and remove all of your sensitive/important data and apps from your cellular device

How To:

iOS
1. Open iTunes and connect your device to your computer.
2. If a message asks for your device passcode or to Trust This Computer, follow the onscreen steps.
3. Select your iPhone, iPad, or iPod when it appears in iTunes.
4. If you want to save Health and Activity data from your iOS device or Apple Watch, you need to encrypt your backup: Select the box called Encrypt [device] backup and create a memorable password. If you don't need to save your Health and Activity data, you can make a backup that isn't encrypted. Just click Back Up Now.
5. When the process ends, you can see if the backup finished successfully on the Summary screen in iTunes. Just look under Latest Backup to find the date and time.

Android
1. Connect your phone to your computer via a USB cable, and it will show up as an external hard drive. For Macs, you may need to first download a tool called Android File Transfer.
2. Select the disk, and navigate to the DCIM folder. This folder contains your video and picture data.
3. Select the other data files that you want to back up, and drag them to an area on your computer, such as your desktop. The selected files will copy over to your computer.

Optional:
☐ Perform a complete factory reset on your cellular device and keep it as barebones as possible.

☐ Ensure all phone updates, including applications, are applied.

How To:

Android OS Updates
▪ Settings > System updates > Download updates manually

Google Play Updates
▪ Select the menu button > My apps & games > Verify all apps are up to date

iOS OS Updates
▪ Settings > General > Software Update

iOS App Updates
▪ Launch the Appstore > Select Updates

SHADØW
SYND1CATE

Tips

Safe Surfing & Messaging:

While at the Cons, it is recommended that you keep all sensitive tasks, conversations, etc. to a minimum or better yet, not at all. The less opportunity you provide for the chance of sensitive information to be potentially accessed by an unauthorized user or stolen, the better. In the case that you may need to perform a sensitive web searches, connect and authenticate to a website, or send sensitive messages, the following are recommended:

- ❖ Utilize a VPN
  - ▪ A VPN will transfer your traffic within secure encrypted tunnels.
- ❖ Refrain from connecting to unknown Access Points (AP)
  - ▪ Instead of connecting to random APs utilize your cellular network data plan on your phone.
- ❖ Utilize a secure messaging app for communication
  - ▪ SMS can be intercepted via an IMSI catcher and the encryption downgraded and cracked. Utilize a secure messaging platform like WhatsApp that provides end-to-end encryption.

Charging:

Although this kind of goes without saying, we want to stress the importance of bringing and using your own chargers! While at the Cons, you will notice a ton of open USB ports mounted on walls or in kiosks as "Cell Phone Charging Stations". Never plug your phone into them to charge! Even though these are built into the wall or are attached to a fancy kiosk, it is trivial to open the panels and embed a device to either maliciously steal data off of your phone, or upload malware to it.

- ❖ Bring your own charger to the Cons
- ❖ Bring a portable charger, for power on the go!

Wireless:

The easiest way to get your cellular device pwned or data sniffed while at the Cons is to keep all of your wireless capabilities enabled. With constant zero-days being discovered, vulnerabilities lingering, and unsecure apps sending sensitive information over the wire unencrypted, it is vital that you leave as little of a footprint as possible.

- ❖ Disable Wireless on your phone when not it in use!
- ❖ Disable Bluetooth
- ❖ Disable NFC

Something important to note is that some devices require you to actually go within the main settings section to completely shut off wireless features. As an example, for iOS devices, simply shutting off wireless and Bluetooth within the "Control Center" (Which is drawer that appears when you swipe from the bottom up) does not completely shut off the services. You need to go through the settings panel to completely shut it off!

SHADØW
SYND1CATE

Upon Return:

Lastly, once the Cons are over and it is time to get back to your normal life, you want to completely format and restore your phone as a last cautionary method. In the chance that your device managed to get compromised, completely wiping your system and rebuilding from a known good image should rid it of any ailments.

Another thing to keep in mind, if you end up using a VPN you will want to consider resetting any password or certificates that you used for the VPN connection just in case they somehow managed to get compromised. If you plan on using a personal VPN device, such as your home router with VPN capabilities, prior to utilizing at the Cons ensure it is completely patched with the latest firmware updates that the vendor has available. Although your data is safe and encrypted while within the encrypted VPN tunnel, the header information such as the destination IP address is still readable which could lead to a malicious adversary scanning that IP hoping to find a vulnerability on your VPN device that they can exploit.

Laptop Preparation Checklist & Tips

Preparation Checklist

☐ Backup or create a system image and remove all of your sensitive/important data and software from your laptop

How To:

Windows Backup
- ❖ Select the **Start** button then search for "**Control Panel**" and select it > **System and Maintenance** > **Backup and Restore**
- ❖ Select **Set up backup**, and then follow the steps in the wizard

Windows System Image
1. Select the **Start** button then search for "**Control Panel**" and select it > **System and Maintenance** > **Backup and Restore**
2. In the left pane, choose **Create a system image**, and then follow the steps in the wizard

macOS Backup & Image Utilizing Time Machine
1. Open Time Machine preferences from the Time Machine menu in the menu bar. Or choose **Apple** menu > **System Preferences** > **Time Machine**
2. Click **Select Backup Disk**, **Select Disk**, or **Add or Remove Backup Disk**
3. Select a backup disk from the list, then click **Use Disk**

Optional:

☐ Perform a complete factory reset on your laptop and keep it as barebones as possible.

OR

☐ Use a separate hard drive entirely that is dedicated for the conferences

---

☐ Ensure all OS and software updates are applied

How To:

Windows
1. Click on the Start Menu > Select **Settings** > Select **Update & Security** > **Check for Updates**

   OR

2. Open up the command prompt (Press the Windows + R key simultaneously) and type in the following: **explorer ms-settings:windowsupdate**

macOS
- ▪ Open the App Store > Select **Updates**

Preparation Checklist Cont...

☐ Enable and configure the system firewall to "Deny" by default and allow by exception

How To:

Windows – Turning on Firewall

❖ Select the **Start** button then select **Settings** > **Update & Security** > **Windows Security** > **Firewall & network protection** > Select the "active" profile in use > Ensure "Windows Defender Firewall" is set to **On**

Windows – Tuning the Firewall

1. Select the **Start** button then select **Settings** > **Update & Security** > **Windows Security** > **Firewall & network protection** > Select **Advanced Settings**

2. Verify that in the "Overview" panel that "Inbound connections that do not match a rule are blocked" has a red block symbol showing

3. Review you "Inbound Rules" by selecting **Inbound Rules** from the left panel and ensure that all unnecessary inbound rules are disabled (i.e. unused software rules)

macOS - Turning on Firewall

❖ Select **Apple** menu > **System Preferences** > **Security & Privacy** > **Firewall**

macOS - Tuning the Firewall

1. Select **Apple** menu > **System Preferences** > **Security & Privacy** > **Firewall**
2. Select **Firewall Options** > Select **Block all incoming connections**

3. Select **Automatically allow downloaded signed software to receive incoming connections**

4. Select **Enable stealth mode**

Tips

🌐 Safe Surfing:

While at the Cons, it is recommended that you keep all sensitive tasks, conversations, etc. to a minimum or better yet, do not conduct any sensitive tasks at all. The less opportunity you provide for the chance of sensitive information to be potentially accessed by an unauthorized user or stolen, the better. In the case that you may need to perform sensitive web searches, connect and authenticate to a website, or send sensitive messages, the following are recommended:

- ❖ Utilize a VPN
  - ▪ A VPN will transfer your traffic within secure encrypted tunnels.
- ❖ Refrain from connecting to unknown Access Points (AP)
  - ▪ Instead of connecting to random APs utilize your cellular network by tethering your phone to your laptop.

🔒 Encryption:

If you decide that you do not want to go through the hassle of backing up your data and wiping and rebuilding your system with a fresh barebones image, then at least consider encrypting your sensitive information. It is recommended that you encrypt your entire hard drive (full disk encryption) as well as encrypt individual sensitive files.

The reason why you want to utilize both forms is because each will provide their own security benefits. Full disk encryption encrypts the entire disk preventing a thief from stealing your laptop and attempting to gather information off the hard drive. However, on the flip side of that, let's say that your laptop is on and unlocked therefore already in a decrypted state. The thief would now have access to all the unencrypted data. On the other hand, with the use of file encryption, even when your system is online and unencrypted, file encryption allows you to encrypt specific files which remain encrypted until each are individually unlocked. You will at least have peace of mind that if your system is compromised and data exfiltrated your sensitive data will be in an encrypted and unreadable state.

- ❖ macOS systems, utilize the built-in FileVault for full disk encryption
- ❖ macOS systems, utilize the Disk Utility for individual file/folder encryption
- ❖ Windows systems, utilize the built-in BitLocker for full disk encryption
- ❖ Windows systems, utilize EFS for file/folder encryption

📶 Wireless:

The easiest way to get your laptop pwned or data sniffed while at the Cons is to keep all of your wireless capabilities enabled. With constant zero-days being discovered, vulnerabilities lingering, and unsecure apps sending sensitive information over the wire unencrypted, it is vital that you leave as little of a footprint as possible.

- ❖ Disable Wireless on your phone when not it in use!
- ❖ Disable Bluetooth
- ❖ Disable NFC
- ❖ Disable RF
- ❖ Disable Infrared

SHADØW
SYND1CATE

Upon Return:

Lastly, once the Cons are over and it is time to get back to your normal life, you want to completely format and restore your laptop as a last precautionary method. In the chance that your device managed to get compromised, completely nuking your system and rebuilding from a known good image should rid it of any ailments.

Another thing to keep in mind, if you end up using a VPN you will want to consider resetting any password or certificates that you used for the VPN connection just in case they somehow managed to get compromised. If you plan on using a personal VPN device, such as your home router with VPN capabilities, prior to utilizing at the Cons ensure it is completely patched with the latest firmware updates that the vendor has available. Although your data is safe and encrypted while within the encrypted VPN tunnel, the header information such as the destination IP address is still readable which could lead to a malicious adversary scanning that IP hoping to find a vulnerability on your VPN device that they can exploit.

BSidesLV Guide

Overview

🌐	**Website:**	https://www.BSidesLV.org
📅	**When:**	August 7th-8th
📍	**Where:**	Tuscany Suites 255 E Flamingo Rd, Las Vegas, NV 89169
💵	**Cost:**	FREE!

Background:

BSidesLV can be beautifully summarized by the following quote that can be found directly on their website:

> "BSides Las Vegas is an Information / Security conference that's different. We're a volunteer organized event, put on by and for the community, and we truly strive to keep information free."

BSidesLV is celebrating their 10th annual conference in 2018, having hosted their first conference back in 2009. BSidesLV is a free conference and is extremely welcoming to newcomers in the field as well as seasoned veterans.

Things to Do:

BSidesLV provides a plethora of things to do while at the conference. Below is a quick highlight of some of the things to look out for while at the con:

- ❖ Networking/Socializing
- ❖ CTF
- ❖ Tracks
- ❖ Parties/Events

We will dive in a little further as to what the above points entail of.

Things to Do

Networking/Socializing:

Networking/Socializing with your fellow cyber folks is arguably one of the most important aspects in the cybersecurity field. By networking/socializing, you can gain an amazing amount of information and build lasting relationships that can be used to help you advance in your career. This is one of the best things about BSidesLV. It is smaller than DEF CON and Black Hat so you get a more personable experience allowing you an amazing opportunity to network with people.

CTF:

BSidesLV hosts the "Pros vs Joes" Capture the Flag (CTF) every year. This is an awesome opportunity for you to work together on a team with fellow cyber enthusiasts and learn valuable Tactics, Techniques, and Procedures (TTPs) that you can directly use in the field. This CTF is unique, in that not only do you get to go hands-on the keyboard and hack away, but you also get to work alongside "Pros" and learn as you go! Registration for this is usually in May. If you are interested in playing next year, follow @dichotomy1 on Twitter and you'll know when registration opens. Another thing you can do is keep tabs on the website as they usually announce it there too!

Tracks:

BSidesLV has a bunch of different tracks, and some of them go on at the same time. These tracks cover a variety of security topics and there is something for everyone! The tracks you can expect to find this year as well as their description as stated on the BsidesLV website is as follows:

- ❖ Breaking Ground
    - ▪ Ground Breaking Information Security research and conversations on the "Next Big Thing". Interactively discussing your research with our participants and getting feedback, input and opinion. No preaching from the podium at a passive audience.
- ❖ Common Ground
    - ▪ Other topics of interest to the security community. e.g., Lock-picking, hardware hacking, mental health/burnout, Law, Privacy, Regulations, Risk, Crypto, Activism, etc. Again, interactive discussions with your peers and fellow researchers. Not passive lectures "at" an audience.
- ❖ Ground1234!
    - ▪ Focused on the (in)security of passwords and other authentication solutions, bringing together security researchers, password crackers, and experts in password security from around the globe in order to better understand and address the challenges surrounding digital authentication. This track explores all facets of authentication security, from analysis and education to creating, securing, cracking, and exploiting authentication solutions.
- ❖ Ground Floor
    - ▪ Foundational talks on topics relevant to security practitioners today.
- ❖ Ground Truth
    - ▪ Focused on use of data science, statistics, and other analytics techniques to solve problems in infosec.

❖ Hire Ground
  ▪ Our 2-day Career Track focusing on resume review, career planning and tracking, interviewing tips and tricks and getting you directly in front of companies that are hiring. Find out what good recruiters are looking for and how to best work with them to further YOUR career!
❖ I Am The Cavalry
  ▪ Security that affects public safety and human life. Where our domain overlaps others, we must gather teammates and forge an alliance. Technical discussions cover medical devices, cars, and other connected technologies with a higher consequence of failure. Non-technical talks cover issues where security overlaps with the human condition, and building skills to influence change outside the echo chamber.
❖ Proving Ground
  ▪ Mentorship and Scholarship track for first time national speakers. Get paired with a great mentor, who will help you with your presentation from CFP to podium AND receive up to $500 to help offset the costs of traveling to Vegas to present.
❖ Training Ground
  ▪ Consists of workshops and classes to give your students hands-on experience learning the latest and greatest. We accept proposals for 1/2 day, full-day and 2-day workshops.
❖ Underground
  ▪ OTR talks on subjects best discussed AFK. No press, no recording, no streaming, no names. Just you and your peers, discussing what matters, behind closed doors. Think about it.

Parties/Events:

BSidesLV is known for their awesome pool parties each year, and this year they will again be hosting it! It will be located at the Tuscany Suites Pool. They will have a party each night and have 24hr control of the sound system at the pool as well!

Another fun event that will take place is none other than a water balloon fight! This will take place on the evening of Tuesday August 7th! It's $20 to participate and an extra $10 if you want to bring a super soaker gun or something like that. Better yet, all the money will be donated to Hak4Kidz! More information about Hak4Kidz can be found here: http://hak4kidz.com

Useful Information

Admission:

Due to the limited space of the venue, as you can imagine, not everyone will be allowed in. BsidesLV offers a few ways to obtain an entry badge. Since they try to stay true to their word on being "Free", you cannot specifically buy a badge however, they do allow you to donate which will land you badge while they last! Below is a listing of the different ways you can obtain a badge and be granted access to the Con:

- ❖ Be selected as a part of the Pros vs. Joes CTF
- ❖ Volunteer for the Con!
- ❖ Donate and receive a donor badge
- ❖ Have your company sponsor the Con
- ❖ Enter and win the Logo or Slogan contest
    - o The contests are held on Twitter a few months before the con
- ❖ Book a 3-night stay at the Tuscany Suites under the BsidesLV room block
- ❖ Submit a talk!
- ❖ Wake up extremely early the day of the Con and wait in line for hours in hopes of snatching one of the limited general admission badges….not recommended…

Volunteering:

One of the unique features of BsidesLV is their openness for volunteers. Volunteering opportunities range from AV Assistant, Info Booth, NOC, and more! Volunteering also comes with a ton of benefits. Like mentioned above, volunteering will grant you a badge for Con access! You get a t-shirt and they also host a volunteer's appreciation dinner so you get recognized. This is one of the best ways to meet new people and get involved with the industry. It also has the added benefit of looking good on your resume too if you're trying to get a job!

Food:

There will be coffee, water, and a bar there. The bar will be free on both days at 5 PM for one hour. Don't forget to tip!

If you bought a food ticket then you get the lunch that they serve there. Otherwise, you can go downstairs to the cafe or restaurants. Alternatively, you can go across the street for lunch. If you are more health conscious, you can bring your own lunch too; just make sure to bring a lot of ice to keep it cool!

Parking:

Parking at the Tuscany Suites hotel is free! This is great because that's not too common nowadays. If you plan on driving there, we do recommend getting there earlier rather than later just to play it safe since their parking lot isn't huge.

DEF CON Guide

Overview

Website: https://www.defcon.org

When: August 9th-12th

Where: Caesar's Palace
3570 S Las Vegas Blvd, Las Vegas, NV 89109
&
Flamingo
3555 S Las Vegas Blvd, Las Vegas, NV 89109

Cost: $280 cash at the door

Background:

DEF CON is the largest and one of the oldest hacker conference in the world! Every year the turnout gets larger and larger to the point they are exceeding maximum occupancy in numerous hotels at once! This year marks the 26th year of the DEF CON conference. As a brief history lesson, based on their websites information, DEF CON originally started back in 1993 and was meant to just be a party for members of "Platinum Net", a Fido protocol based on hacking network out of Canada. It ended up turning into a large event!

The name "DEF CON" stems from a couple of sources. For one, a large majority of the inspiration comes from the movie War Games. DEF CON is also short for "Defense Condition" for those in military. Lastly, "DEF" is #3 on a phone for those who are Phreaks! There is a ton of history when it comes to DEF CON, too much to fully list but as you get more acquainted, you will see just why this conference is the largest and oldest of them all!

Things to Do:

DEF CON is such a massive conference that there are literally too many things to list. With their 26th conference just around the corner, it is slated to be their largest event to date! Below is just a high-level list of things to do while at the con. Like mentioned above, there is too much to list them all so this by no means is all-inclusive:

- ❖ Networking/Socializing
- ❖ CTF
- ❖ Talks
- ❖ Villages
- ❖ Workshops
- ❖ Vendors
- ❖ Parties/Events

We will dive in a little further as to what the above points entail of.

Things to Do

Networking/Socializing:

Networking/Socializing with your fellow cyber folks is arguably one of the most important aspects in the cybersecurity field. By networking/socializing, you can gain an amazing amount of information and build lasting relationships that can be used to help you advance in your career. DEF CON is massive with up to 20,000+ attendees each year. Although it will not be as personable and quaint as BSidesLV, you can expect to see meet hundreds and thousands of people. This includes people who are new to the field, to legends who have been doing this for years!

As a heads-up, not everyone is friendly and outgoing. Some attendees can be flat out rude, so have your thick skin on and don't get discouraged while there. Do your best to meet new people while attending the villages or standing in lines. You never know who you may run into while you are there. If anything, you can always come hangout with the Shad0w Synd1cate crew. We promise we won't bite!

CTF:

There is not just one CTF event at DEF CON, there are numerous different CTFs each specific to the different villages and topics. Below is a list of some the CTFs that will take place during the Con:

- ❖ Social Engineering CTF
- ❖ OSINT CTF
- ❖ Car Hacking Village CTF
- ❖ Wireless Packet Capture CTF
- ❖ Recon Village CTF

On top of the above mentioned CTFs, DEF CON is home to the granddaddy of all CTF events. Each year they hold one massive CTF event that takes place during the majority of the Con. Not just anybody can be a part of it, only the best teams out there! There is a dedicated group, Order of the Overflow, that spends the year preparing and coming up with the most difficult CTF puzzles they possibly can. On top of that, there are qualifier rounds that teams must rank in to actually progress to the final event at DEF CON. It is a lot of blood, sweat, and tears, but the team that comes out number one goes down in history and get the prestigious "Black Badge" granting them access to DEF CON each year free for life!!

Talks:

DEF CON is well known for their incredible talks. A lot of times, these talks are on topics that are extremely new/cutting edge or even better, world premieres of new exploits, vulnerabilities, and sometimes even zero-days!

With so much action going on between the villages, workshops, and talks, one will find it hard-pressed to attend every talk. Have no fear! A majority of the talks end up on YouTube or can be downloaded/streamed from the DEF CON media server located here: https://media.defcon.org/ . For organizations interested in purchasing the talks, they also sell them bundled with the BlackHat talks!

Since you will more than likely be able to view these talks after the Con online, we recommend you only attend the ones that really intrigue you and leave the rest for streaming later. That way you can indulge on the numerous other things to do around the Con.

Villages:

One of DEF CON's unique traits is their villages. A village is basically an area in the Con that is dedicated to a specific subset of cybersecurity. This year, DEF CON is looking to break a record for the most villages ever, twenty-eight!

Each of these villages is full of a ton of information dedicated to its specific subset. They can almost be seen as different groups where a lot of them nowadays create their own unique badges and host their own CTFs and other events! Below is listing of a few of the many villages that will be there this year:

- ❖ Crypto and Privacy Village
- ❖ Wireless Village
- ❖ Biohacking Village
- ❖ Lockpicking Village
- ❖ Soldering Skills Village
- ❖ Voting Machine Hacking Village

And much more!

For an all-inclusive list on all the villages that will be present this year, go check out the village page located here: https://www.defcon.org/html/defcon-26/dc-26-villages.html . This page also provides a brief overview of the village and what you can expect from it.

Vendors:

Another awesome feature DEF CON has that is worth noting, is a dedicated spot for vendors! And no, we are not talking about the ones that are trying to sign you and your company up for a 10 year multi-million dollar contract. We are talking about the ones that sell some of the hottest hacker gear on the market!

Each year tons of vendors come out to DEF CON and set up stand to sell some awesome merchandise. Some of the vendor you can expect to see there are as follows:

- ❖ HackerBoxes
  - o HackerBoxes is the subscription box service for DIY electronics and hardware hacking.
- ❖ Hacker Warehouse
  - o Hacker Warehouse is your one stop shop for hacking equipment. From WiFi Hacking to Hardware Hacking to Lock Picks, we carry equipment that all hackers need.
- ❖ Hak5
  - o Discover the devices that have found their way into the hearts and tool-kits of the modern hacker. Notable for ease of use. Celebrated by geek culture. From comprehensive WiFi audits to covert network implants and physical access mayhem - Hak5 Gear gets the job done.
- ❖ No Starch Press
  - o Awesome cybersecurity books all at a discounted rate of 30% off!

There are just so many more! Be sure to bring some extra cash to pick up on some amazing gear!

Workshops:

On top of the amazing talks and villages that DEF CON puts on, they don't stop there! They even have fully hands-on workshops! These are targeted for individuals who really want to pick up some new tricks. These workshops last for a couple hours up to nearly an entire day. You can view these as actually training events where you will have a veteran instructor or instructors guide the class and walk you step by step through specific security related topics!

DEF CON workshops are some of the hottest things to do at the con and they RSVP out in a matter of seconds! For those interested in signing up for a workshop next year, they usually open registration about a month before the con. Keep tabs on the website for when the registration date is announced. If you don't register right away, your chances of getting into one of the workshops is very slim. However, something to keep in mind is the fact that many of the villages have their very own workshops. So keep an eye open for them!

Useful Information

Admission (a.k.a. "Line Con"):

This year, DEF CON is renting out space in two massive casinos, Flamingo and Caesar's Palace! With that being said, you won't have the same issue of not being able to get a ticket like what can happen at BSidesLV. However, on the other hand, you will have to deal with what is known as "Line Con". With such a large venue space reserved, there are upwards of 23+ thousand attendees! You can imagine just how long the lines are to get your badge and receive admission.

This is an ideal time to start socializing with some of the fellow attendees and make some new friends! Once you finally reach the end of the line, you will be greeted by one of the volunteers where they will gladly trade your $280 for a fancy DEF CON badge. We recommend you get there as early as possible to avoid being stuck in line for hours!

Volunteering:

Although DEF CON does accept volunteers, their acceptance policy is far more stringent than that of BSidesLV. It usually requires a current "goon" (nickname given to DEF CON volunteers) to recommend you as a potential goon candidate. If you read their about page, there really isn't an application process. They just recommend you talk to a goon about it and go from there!

Food:

At DEF CON, you are pretty much in the dead center of the Las Vegas strip. You will find a mixture of everything here. With that being said, keep in mind that you are on the Las Vegas strip that is driven by money! The cost of everything is increased.

Caesar's has a food court, but it gets busy during lunch! Imagine thousands of people trying to get lunch all at once. We recommend walking across to the LINQ where they have some really yummy fast food restaurants that aren't as busy. We also recommend that you bring some snacks with you. You will be walking, talking, and moving all day. You will be surprised at how hungry you get!

Parking:

One pro to having a conference at a massive venue is that there are also massive parking lots and garages. Between Caesar's and Flamingo there should be plenty of space to park in the garage. However, parking at Caesar's or Flamingo will cost you around $12 a day. Another option is to leverage the Las Vegas Strip's monorail system. The monorail runs up and down the strip making a total of 7 stops with one of those being at Caesars Palace and Flamingo. You can easily park your vehicle at one of the casinos further away and take the monorail to beat out the traffic!

General Tips

Tips

On top of the recommended preparation tips for your cell phone and laptop, below is a list of some other general tips that we recommend you be cognizant of!

RFID Shielding:

If you plan on carrying any of your debit/credit cards or anything else that utilizes RFID, you are going to want to make sure they are safely secured within an RFID shielded bag or wallet. Even though RFID tags are only supposed to be readable up to a few feet, it has been demonstrated that customized readers can detect RFID tags from upwards of 60+ feet. If you can't keep the cards at home then make sure they are properly being shielded!

Cash:

Make sure that prior to going to the Cons you pull out cash from your bank. Refrain, I repeat, refrain from using any of the ATMs at the Cons. There have been instances in the past where a fake ATM machine was placed within the conference. Also, skimmers are another thing to watch out for. Just play it safe and go to your local bank for cash withdrawals!

QR & NFC:

While walking around the Cons, you may run into some random QR codes or NFC tags laying around. Do not just openly scan/connect to them! It is trivial for a malicious link or file to be embedded within them causing your device to be directed to a malicious site or automatically download a malicious file leading to your device being compromised. Like anything, know what you are scanning/connecting to prior to doing it. If you have anything that may be sensitive on the device you are using, don't take the risk!

External Storage:

Last but not least, external storage devices. This usually goes without being said, but it needs to be mentioned anyways! Be cognizant of any USB drives, CDs, etc. that may be laying around the Cons or even given to you. You have no clue where it has been and what may be on it. If it didn't come from a trusted source, do not take the chance and plug it in!