1. GİRİŞ

Bu yazının amacı, her yıl Amerika'nın Nevada eyaletinin Las Vegas şehrinde düzenlenen BlackHat [1] ve hemen sonrasında düzenlenen DefCON [2] hacker ve güvenlik konferansının içeriği ve adım adım konferansa ve etkinliklere katılım hakkında bilgi vererek gitmek isteyenlere bir rehber oluşturmaktır. Bu sene (2014) Blackhat ve DefCON'a katılmamı sağladığı için şu an çalıştığım şirkete (STM A.Ş) ayrıca teşekkür ediyorum.

2. BLACKHAT Hacker ve Güvenlik Konferansı

Blackhat hacker ve güvenlik konferansı siber güvenlik alanında çalışan kişilerin katılması gereken bir numaralı güvenlik konferansı diyebiliriz. Buraya katılmak için:

- ✓ Öncelikle kendinize bir sponsor bulmanız veya ücretleri kendiniz karşılamanız gerekiyor. Tabi bir sunum ile konferansa konuşmacı olarak katılmıyorsanız. Konferansta bir sunum, bir uygulama tanıtımı olmak üzere 3 Türk arkadaşımızın sunumu vardı. Gururlandık.
- ✓ Konferansa katılırken hangi pozisyonda katıldığınız önemli. Aşağıdaki tablo, geçiş tiplerine göre hangi etkinliklere katılabileceğinizi göstermektedir. Ben, 2 günlük bir eğitime katılmıştım. Aşağıdaki tabloya göre benim briefing'lere ve keynote konuşmalarına katılamam gerekiyordu. Fakat katılabildim ve herhangi bir engel olmadı. Sadece Offensive Security'in sponsored bir workshop'u vardı (Kali Linux Workshop), ona katılamadım. Ayrıca blackhat konferansına ilk gidenler arasındaydım, gittiğimde daha yeni hazırlıklar yapılıyordu.

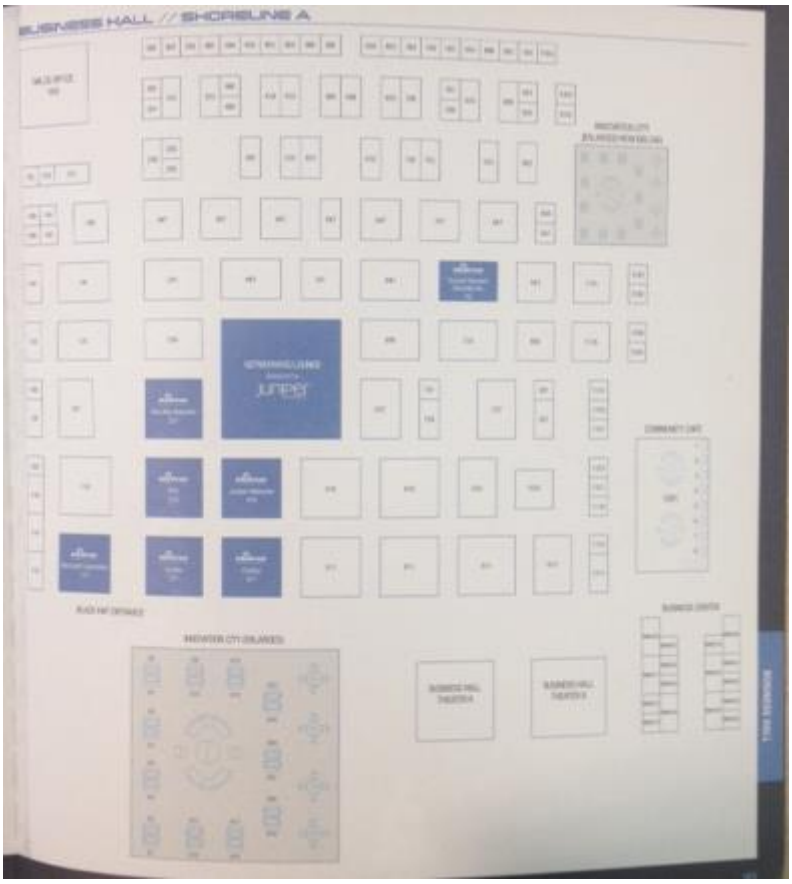
PASS COMPARISON CHART

Pass Types	Briefings Only	Briefings & Trainings	Trainings Only	Business Pass
Access to Briefings	X	X		
Access to Training		X	X	
Access to Keynote	X	X		
Access to Business Hall	X	X	X	X
Access to Sponsored Workshops	X	X	X	X
Access to Sponsored Sessions	X	X	X	X
Access to Arsenal	X	X	X	X

- ✓ Siz, sadece briefinglere katılım için gidebilirsiniz. Fiyatlar erken kayıt olup olmamasına göre değişiyor. Tavsiyem erken kayıt yaptırın, zaten yüksek fiyatlar ve tabi uçak bilet fiyatları.
  Fiyatlar (2014):
  - Businness Pass:495$ (limitli)
  - Briefings: 1795-2595 arası
  - Trainings: 2000-4500 arası (eğitimden eğiteme değişiyor)

- ✓ Kayıt olurken ayrıca DefCON bileti de alabiliyorsunuz. 220$ değerinde. Tavsiyem blackhat konferansından sonra düzenlenen DefCON'a katılacaksınız burada işaretlemeniz.
- ✓ Kayıt olduktan sonra size bir doğrulama emaili geliyor. Fatura göndermiyorlar. İstemeniz gerekiyor. Sonra hemen düzenleyip gönderiyorlar.
- ✓ Bundan sonra Las Vegas'ta nerede kalacağınıza karar vermeniz gerekiyor. Zaten çok otelde durmayacağınız için orta karar bir yer yetiyor. 2014 Etkinliği Mandalay Bay'da olmuştu. Tavsiyem uygun yollu bir otel bulun ve araba kiralayın. Çünkü sadece konferans yok☺ Alışveriş yapmak ve konsept otelleri gezmeniz için akşamlar sizin. Ayrıca DefCON konferansı da ayrı bir otelde olduğundan otel falan değiştirmenize gerek kalmaz. Bu şekilde daha uygun olduğunu düşünüyorum.
- ✓ Las Vegas'ta Maccaran havaalanı uluslararası bir hava alanı ve çok büyük. Uçaktan indikten sonra otobüs ile araba kiralama yerlerine gidip araba kiralayın. Economy class bir araba 9 gün için 500-600 tutuyor.
- ✓ Konferansa bir gün önceden gelmeniz yerinde olur. Erkenden kayıt yaptırırsınız, hiç sıra olmuyor. Konferans günü kuyruk çok uzuyor.
- ✓ Konferansa kayıt yaptırdığınızda size konferans rehberi veriyorlar. Bu rehberde:
  - Konferansla ilgili harita
  - Konferans programı
  - Konferans konuşmacı ve katılımcıları bilgileri

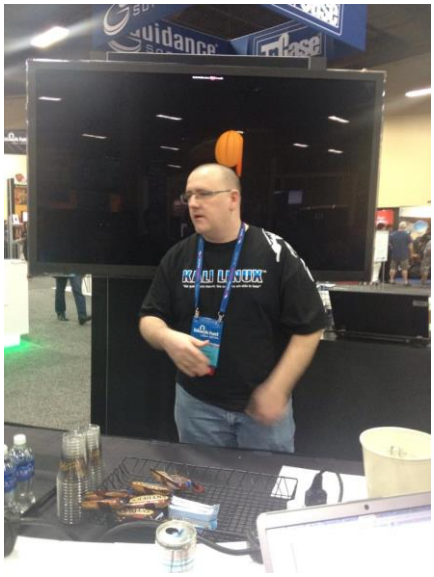
- ✓ Blackhat için ayrıca mobile uygulama da yapılıyor. Bunu kullanmanız çok önemli. Çünkü konferans çok büyük ve ilgilendiğiniz sunumları ve araçları buradan işaretleyip kendi takviminize ekleyebiliyorsunuz ve böylelikle ilgilendiğiniz etkinliklerden zamanında haberiniz oluyor.
- ✓ Ben bir eğitime katıldım. Eğitimler konferanstan önceki 4 gün içerisinde yapılıyor. Eğitime katılanlara yemek, kahve ve atıştırmalıklar dahil. Maalesef konferans sırasında yemek yoktu. Kendiniz bir şekilde karnınızı doyurmanız gerekiyor, tabi bunun için yerler mevcut.
- ✓ Konferansta 6 bölüm var diyebiliriz:
    - **Arsenal: (Bussinness Hall)**
        - Burası firmaların ürünlerini ve kendilerini tanıttıkları çok geniş bir alan.(Rapid7, Tenable, Microsoft, Cisco, Checkpoint, Symantec, vb)
        - Ayrıca çeşitli etkinliklerin (CTF, oyunlar, hediyeler, vb.) olduğu bir yer☺
        - Katıldığım bir wireless CTF'den Amazon'dan 25$'lık hediye kartı kazanmak ayrıca sevindirdi. Buna da amazondan kitap sipariş ettim. Amazon hakkında da şunu belirtmek faydalı olacaktır. Amazonun Prime üyeliği var ve 1 ay deneme süresi bedava. Buraya üye olursanız eğer alacağınız ürün prime özellikli ise 2-gün de elinize ulaşıyor. Bunu da dert etmeyin çünkü Blackhat+DefCON 7 gün sürüyor. Oteller her paket için bir teslimat ücreti alıyor bu da 3-7 arasında değişiyor.
        - Burada ayrıca kitap imzalama (kitabın yazarının bizzat imzaladığı ve bedava verdiği örn:anti-hacker toolkit kitabını imzalı olarak bedavaya dağıttılar), yeme içme zamanları oluyor. Tabi bunları denk getirmeniz gerekiyor.



- **Uygulama Tanıtımları:**
  - Toolswatch sponsorluğunda güvenlik camiasında kullanılan araçların bizzat geliştiricileri tarafından tanıtıldığı bir alan.
  - Volatility, Owasp zap, BeEF, Dradis, ProxyMe, vb bildiğiniz araçları bizzat kendi geliştiricilerinden görmek hoş oluyor.
  - Tubitaktan Heybe sızma aracının yazarları olan Gökhan Alkan ve Bahtiyar Bircan da buradaydı. Ayrıca gurur kaynağımızdı. Konferansta 10'a yakın Türk vardı. Buna sevinmeli miyiz yoksa üzülmeli miyiz bilemedim ☹
- **Sunumlar:**
  - Konferansta birçok sunum var ayrı ayrı yerlerde ve paralelde gerçekleşiyor.
  - Bu sebepten çok iyi hazırlanmalı ve daha önceden nereye katılacağınıza karar vermeniz gerekiyor.
- **Sponsored Workshoplar:**
  - Markaların yapmış olduğu çalışmalar ve sunumlar.
  - Kaizen CTF'e katıldım. Çok eğlenceliydi. Havayı solumak bile güzeldi ☺
  - Ayrıca B2B toplantılar yapılıp, iş geliştirme faaliyetleri de yapılıyor.
- **Blackhat Dükkanı☺**
  - Burada blackhat konferansı ile ilgili hediyelik eşyalar bulunmakta.
  - Anı için belki bir tshirt, belki bir çıkartma alabilirsiniz.

- **Kitapçı:**
  - Burada güvenlik ile ilgili kitapların son versiyonlarını bulabilirsiniz.
  - Ayrıca imza günleri oluyor ve kitapların yazarlarına imzalatabiliyorsunuz.

✓ Konferansta güvenlik camiasında tanınan isimleri bizzat görmek de ayrıca değişik bir tecübeydi. ISC2 başkanı Hord Tipton, Kevin Mithnick ve Offensive Security Kurucularından Mati Aharoni



✓ Akşamları ayrıca bazı grupların (OWASP, ISC2, vb) etkinlikleri oluyor. Bunlara önceden kayıt olmak gerekli. Ben ISC2 etkinliğine katılıdım.

✓ Arsenal'de bazı firmalar akşam için etkinlik biletleri verdiğini de ayrıca belirtmeliyim (Dünyanın ilklerine girmiş clublerin biletleri. Akşam gidip bir görmekte fayda var. Buralarda network yapıp, bağlantılarınızı da artırabiliyorsunuz.)

✓ Konferansın son gününde DefCON biletleri kayıt olanlar için sağlanmaktadır. DefCON'un ilk günü Blackhat'ın son günüyle çakışsa bile DefCON'un ilk gününde pek bişey olmuyor. Asıl açılış blackhat konferansı bittikten sonraki gün oluyor. Zaten her iki konferansın düzenleyeni de aynı, the Dark Tangent lakaplı Jeff Moss[3]

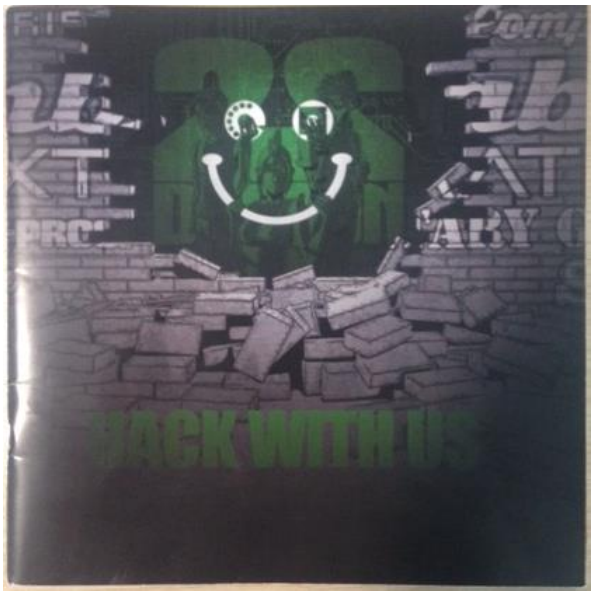
✓ Blackhat konferansı gerçekten görülmesi gereken bir yer. Katılımcıların sonuna kadar faydalanması gerekli olan bir yer. Umarım siz de katılma imkanı bulabilir ve böyle bir ortamı görebilirsiniz.

3. DefCON Hacker ve Güvenlik Konferansı

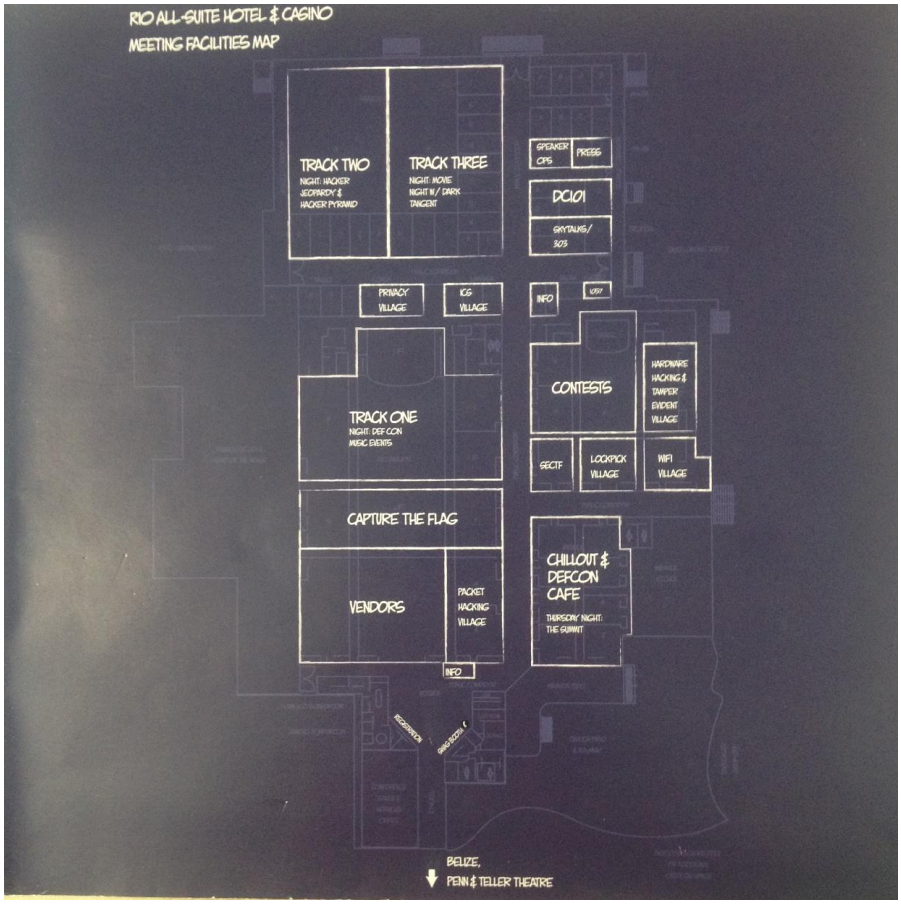
DefCON 22 (2014), blackhat ile karşılaştırıldığında daha çok etkinliği olan bir konferans. Blackhat daha çok güvenlik iş dünyasına, DefCON ise security geekler [4] için bir konferans benim gözümde ve açıkçası DefCON benim daha çok hoşuma gitti.(içimdeki geek ortaya çıktı☺). Rio otelde yapıldı.

Şimdi adım adım DefCON'da yapılması gerekenleri sıralayalım:

- ✓ Blackhat'e kayıt yaptırırken eğer DefCON içinde kayıt olduysanız biletinizi oradan alabildiğinizi söylemiştim. Eğer direkt DefCON'a gidecekseniz (ki bence en azından Türkiye'den gidenler için Blackhat+DefCON yapmak en uygunu) açılış günü sıraya girip alıyorsunuz.
- ✓ DefCON 220$ olduğu için katılım çok yüksek bu sebepten çok sıra oluyor her yerde. Bu sebepten kayıt esnasında size verilen kitapçığı iyi incelemeli sonrasında da katılacağınız etkinlikleri iyi belirlemeniz gerekiyor. Ayrıca bir de size ilginç bir badge veriyorlar, içerisinde gizemler barındıran.
- ✓ Badge'in bir usb girişi var. Terminal ile bağlanıp içerisinde gizlenen kodu kırabilir, ayrıca kendi kodunuzu çalıştırıp, kart üzerindeki ledlerin yanış şekillerini değiştirebilir, üzerine monte ettiğiniz cihazları yönetebilirsiniz. Bir katılımcı, bu badge ile kendi tasarladığı led panel üzerinde top tutmaca oyunu yazmıştı...



- ✓ DefCON haritası yukarıdaki gibidir. Şimdi bu haritadan konferansın içeriğini anlatayım:



  - **CTF Alanı:** Burası dünyanın en büyük CTF'i. 16 takım katılmıştı, 8 takımın uzak doğulu olduğunu belirteyim. Burada fotoğraf çekmek yasak. Sadece izleyebilirsiniz. Ama internette bazı fotolar mevcut☺. CTF'de ekipler hem adımları geçip bayrakları toplamaktan hem de kendi portallerini korumaktan sorumlular. Kendi portallerine saldırı olduğunu savunamazlarsa eksi puan alıyorlar. İzlemek ve düzenekleri görmek eğlenceli. Ağırlıklı olarak Mac kullanmaları da ayrıca dikkatimi çekti. Kazanan 0xffa ekibi oldu.

- Village(Köy) denilen alanlar oluşturulmuş ve bu köylerde tek bir konsept işlenmekte
  - **Hardware Hacking Village:** Burada size bir lab ortamı oluşturulmuş. Havyadan tutun, pastasına, büyütecine kadar her şey sağlanmış. Burada isterseniz DefCON badge'ini modifiye edebiliyor yada 20$ a satın alacağınız bir hardware paketini burada birleştirebiliyorsunuz. Oluşan cihaz sonra mors alfabesini anlayan ve konuşan bir cihaza dönüşüyor ve diğer cihazlarla iletişime geçebiliyor. Ben de kendi çapımda badge'i oraya koyulmuş eski bir Ethernet kartının ledlerini sökerek modifiye ettim ve led yanma şeklini değiştirdim. Burası da çok eğlenceliydi ve keyif aldım. Ayrıca kartı bir ara bozdum, burada tekrar lehimleyince düzeldi.

- **Temper Evident Village:** Burası da çok ilginçti. Size mühürlü olarak gelen paketleri nasıl açacağınızı öğretiyorlar ve lab ortamında deneme şansınız oluyor. Bir kaç deneme yaptım gerçekten de metodlar işe yarıyor.

- **Wifi Village:** Burada kablosuz ağlarla ilgili sunumlar ve CTF mevcut. CTF'e katıldım ama bişey yapamadım, sebebi ise katılanlar genelde grup olarak katılmışlar ve daha önce görmediğim tipte düzenekleri vardı. Ayrıca CTF'de her şey serbest olduğundan atak da yiyordunuz ve ortada deauth paketleri uçuşuyordu. Burada boyumun ölçüsünü aldım. Bununla birlikte ortamı görmek arkadaşların düzeneklerini incelemek bile güzeldi.

Ayrıca otelde seyyar access point ile dolananlar bulunuyor. Elinde anten olan katılımcılar bunları bulmaya çalışıyor. CTF kapsamında böyle bir senaryo da mevcut.

- **Lockpick Village:** Burada pinli kilitlerin nasıl açıldığını öğreniyorsunuz ve hatta deneyimliyorsunuz. Bunun için devamlı sunumlar yapılıyor. Ben 5 pin'e kadar açabildim. İsterseniz lockpicking toolkitleri satılıyor. Başlangıç fiyatı 20$ ve özelliklerine göre artıyor. Eğlenceli bir köy.

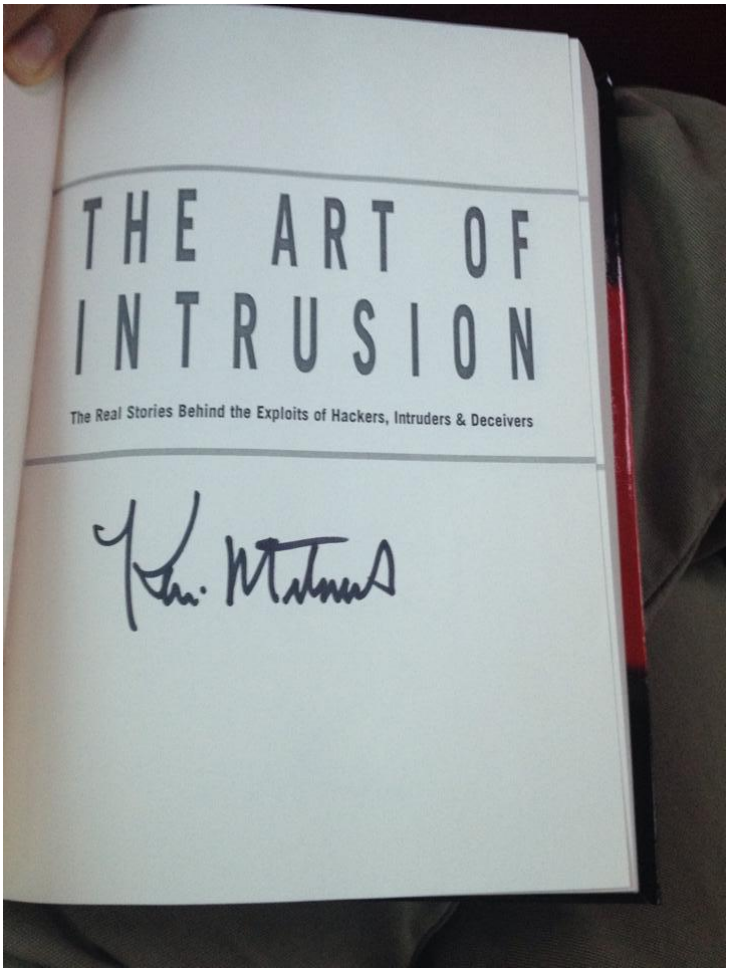
- **Packet Hacking Village:** Burada bir lab ortamı oluşturulmuş ve isteyen verilen senaryolara göre wireshark inceleme yapabiliyor. Lab ortamı basit. Ayrıca bir de CTF var 1 saatlik. 1 saat içinde verilen senaryoların hepsini yapana BlackBadge denilen bundan sonraki bütün DefCON'lara bedava girmenizi sağlayan bir badge veriliyor. Etrafta böyle tipler görebilirsiniz. Ayrıca burada çok ilginç devasa bir ekran var: Wall of Sheep. Neyi gösteriyor derseniz DefCON'da plain olarak wireless üzerinden bağlanılan kişilerin kullanıcı adı ve şifresi gösteriliyor. Şifrelerin birazı maskeli olarak verilse de tahmin edilebiliyor. Katılımcılarda buranın bol bol fotoğrafını çekiyor, ben dahil ☺

- **SeCTF:** Burası social engineering için ayrılmış. Katılımcılar ses geçirmez bir oda içerisinde gerçek yerleri telefon ile arayıp onlardan kendilerine verilen senoryalar kapsamında bilgi alıyorlar ve bunun sonrasında bir rapor oluşturuluyor. Bu CTF'e denek olarak katılan firmalar gerçekten büyük firmalar ve kendilerinin bu tip ataklara karşı ne kadar savunmasız olduklarını görmek istiyorlar. Burası görülmesi gereken bir yer.

- **CONTESTS:** Burası büyük bir alan. Alanın kenarlarına koyulmuş masalarda ayrı ayrı konular işlenmekte:

- OpenCTF, Lockpicking yarışması,vb. Etkinlikler, değişik yarışmalar mevcut.

- Bunların dışında kitapçıkta açıklanan birçok eğlenceli etkinlik bulunuyor.
- **Sunumlar**:
  - Sunumlara talep çok fazla bu sebepten dolayı giremeyebilirsiniz. Girmek istediklerinize 20 dk önceden sıraya girmeniz tavsiye olunur.
  - Blackhat'teki sunumların bazıları burada da gösteriliyor.
- **Skytalks**:
  - Bu sunumlarda fotoğraf ve ses kaydı yasak. İlginç konulardan bahsediliyor. Sadece not alabiliyorsunuz. Diğer sunumlardan çok daha faydalı bence.
- **Satış Alanı:** Burası değişik ürünlerin ve kitapların satıldığı bir alan. Buradan Hak5 wifi pineapple aldım. Ayrıca Kevin Mitnick'in "Art of Intrusion" ve "Ghost in the wires" kitabını aldım ve bizzat kendisine imzalattım ☺



- Ayrıca Defcon20 ile ilgili bir belgesel var [5]. İzlemenizi tavsiye ederim.

- DefCON'da aynı zamanda akşamları partiler oluyor. İnsanların kaynaşması için, oyun oynaması için ortamlar hazırlanmış oluyor. Örneğin neredeyse 3 metrelik langırt, atari konsolları (rubbish monster, vb). Kısaca eğlenceli ve bir o kadar da öğretici bir konferans. Çok şey yapmak isterseniz çok şey yaparsınız, hiçbir şey yapmayıp boş boş da dolanabilirsiniz. Çekinmeyin, sorun, araştırın, etkinliklere katılın…

4. SONUÇ

Bahsettiğim konferanslara dünyanın dört bir tarafından katılım olmakta. Konferansların Las Vegas'ta olması insanın aklına hemen oraya gidenlerin gezmeye eğlenmeye gittiğini aklına getiriyor olabilir. Aklı başında olan her güvenlikçi buradaki ortamı en iyi şekilde değerlendirmeyi ve maksimum faydayı almayı bilir. Türkiye'nin bu gibi yerlere katılımlarının artırması ve güvenliği bürokrasiden arındırıp daha dinamik hale getirmesi gerekiyor. Şirket yöneticilerinin de bu gibi konferanslara katılım yapmanın önemini anlaması gerekiyor.

Ben bu konferanslara katıldığım için son derece memnunun ve maksimum fayda ile geri döndüm. Şimdi ise bu yazı ile sizlere ufacık bir faydam dokunduysa ne mutlu bana.

KAYNAKLAR

[1] https://www.blackhat.com

[2] https://www.defcon.org

[3] http://en.wikipedia.org/wiki/Jeff_Moss_%28hacker%29

[4] http://en.wikipedia.org/wiki/Geek

[5]https://www.google.com.tr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB0QtwIwAA&url=http%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3DrVwaIe6CiHw&ei=pUt4VPfNJuPOygOvyIDQCQ&usg=AFQjCNHC4xD4JS37tUmre-o_zUGKnX5SSA&sig2=U4s-CkZ3wo4xt8iNl8xXIA&bvm=bv.80642063,d.bGQ