HAZIRLAYAN
BEDRİ SERTKAYA
bedri@bedrisertkaya.com
Sistem Uzmanı
CEH EĞİTMENİ

BİLGİ TOPLAMA YÖNTEMLERİ VE KEŞİF:

Bilgi Toplama Terminolojisi:

Bilgi Toplamanın getirdiği tehditler:

Bilgi toplama Metodolojisi:

- ➔ **İnternet vasıtasıyla bilgi toplama**

- ➔ **Rekabet edilen firmalarla ilgili bilgi toplama:**

- **Ürün – Sattıkları ürünün bizden farklılıkları neler? Bizi geçebilir mi?**
- **Promosyon – Ürünlerinin satışı için sundukları cazip yöntemler neler?**
- **Ürün pazarı – Ürünleri kimlere hitap ediyor. Kimler ilgi gösteriyor?**

- ➔ **Whois sorgulamalarıyla bilgi toplama**
- ➔ **DNS üzerinden bilgi toplama**
- ➔ **Websitelerini takip ederek bilgi toplama**
- ➔ **Eposta ile bilgi toplama**
- ➔ **Google Hacking**

Hedef firma ile ilgili bilgi toplama adımları:

Google,Bing,Yahoo,Yandex vb. Çeşitli arama motorlarında aranabilir.

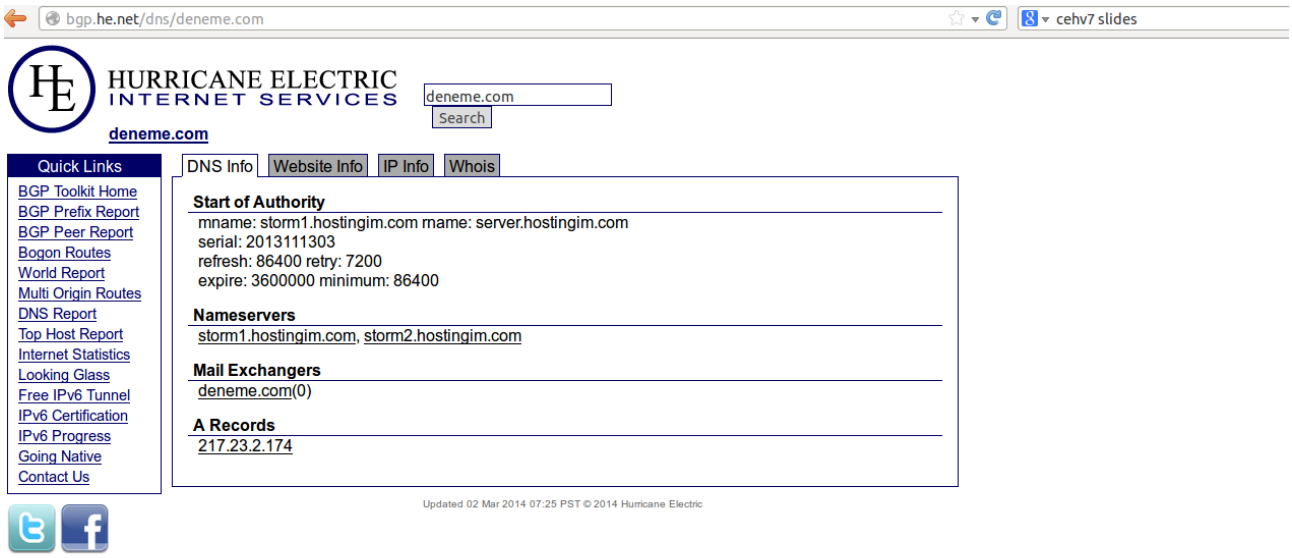
Örnek firma:”deneme.com”

Firmanın alanadı bulunduktan sonra iç alan adları link haritası ve alt alan adları listelenmelidir.

Hedef web sitesinin uptime bilgisi, sunucu çeşidi ile ilgili detaylı bilgiler listelenebilmektedir:
http://news.netcraft.com/

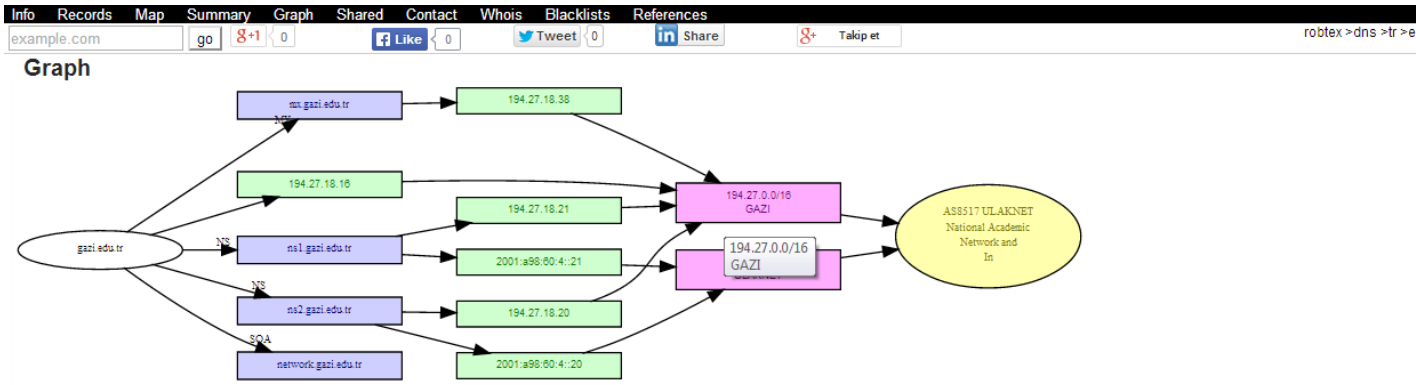
Hedef web sitesinin dns bilgisini,ip aralığını detaylı olarak listeleyen web sitesi:

http://bgp.he.net/



Robtex:

Örnek:https://www.robtex.com/dns/gazi.edu.tr.html#graph



Hedef web sitesinin iç urlleri ve dış bağlantıları listelenebilmektedir:
http://www.webmaster-a.com/link-extractor-internal.php

Alternatif:
http://www.webmaster-toolkit.com/link-extractor.shtml

Hedef şirket hakkında komplike aramalar gerçekleştirilmelidir. Şirket hakkında çalışan listesi, şirket eposta adresleri, linkedin gibi web siteleri üzerinden araştırmalar gerçekleştirilerek toplanabilen bütün bilgiler toplanmalıdır.

Firma Bilgilerini dökmek için kullanılabilecek araçlar:

http://www.webextractor.com

Aynı IP adresinde yer alan adresleri listelemek için bing kullnılabilir:

Derste yaptığımız örnek:
www.bing.com

ping sahibinden.com

çıkan ip sonucu: 85.111.30.111

Bing sorgusu:*ip:85.111.30.111*.

Sorgu ile ip üzerindeki adresler listelenir.

People Search Online Servisleri:

people.yahoo.com

123people.com

wink.com

peoplefinders.com

pipl.com:Derste kullandığımız web sitesi.Sosyal ağlar dahil olmak üzere kişi bilgilerini dökebilmektedir.

Google Alerts(Otomatik arama uyarıları oluşturup eposta adresinize gönderir)

Linkedin

Twitter

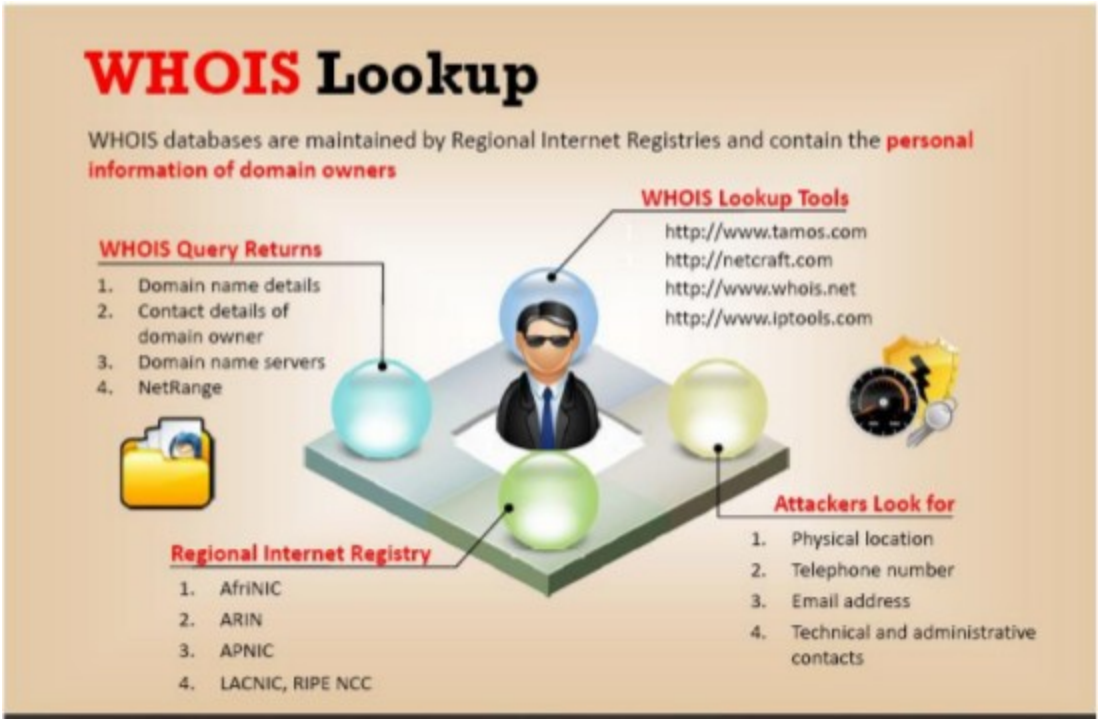
Kariyer.net vb. Iş ilan siteleri

Rekabet edilen firmalarla ilgili bilgi toplama:

Hedef firmaların yaptığı anlaşmalar ve güncel bilgileriyle ilgili döküm çıkaran web siteleri:
Derste incelenen web siteleri:

www.dnb.com
www.sec.gov/edgar.shtml

Whois Sorgulama:



Debian tabanlı ubuntu kali gibi işletim sisteminlerinde whois komutu mevcuttur.

Yüklenmesi halinde kullanılabilir.

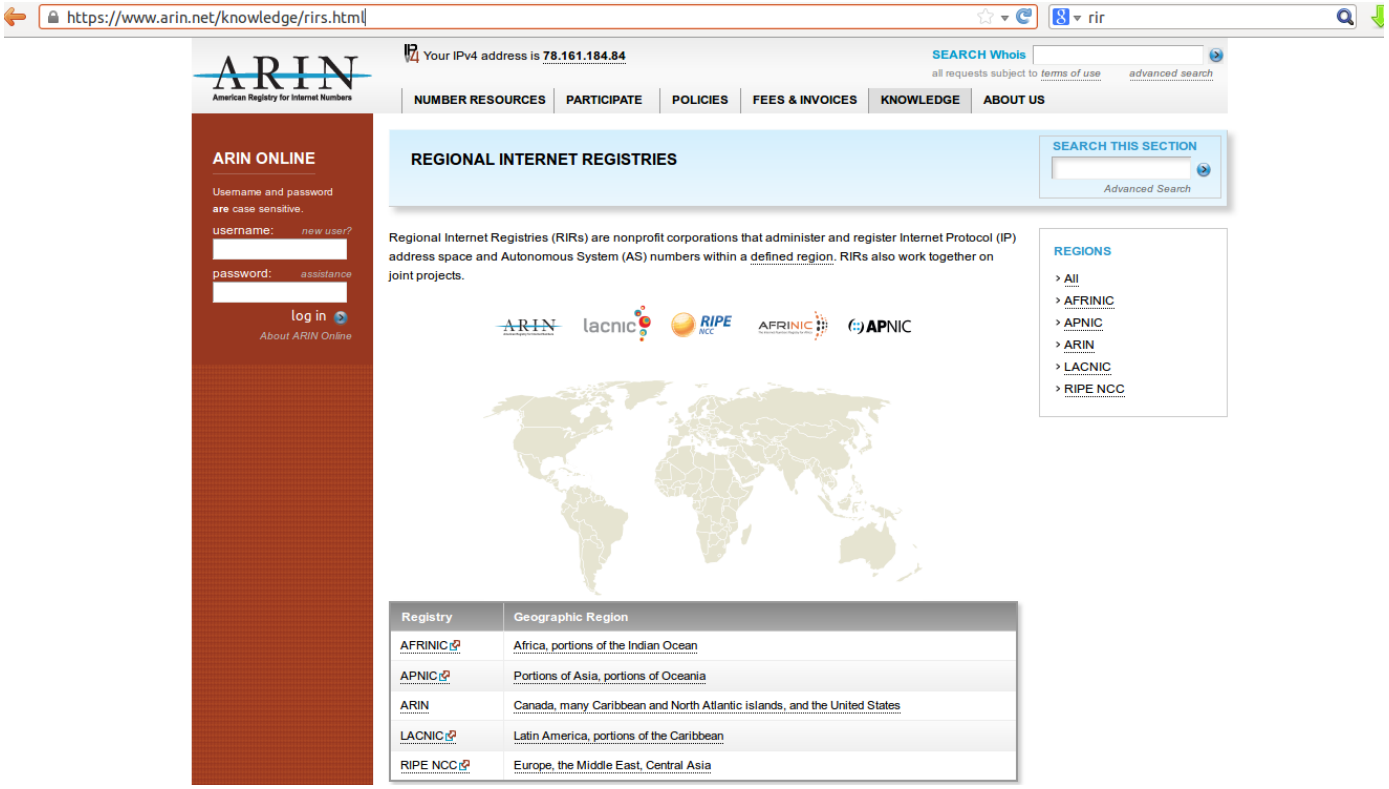
yüklemek için**:apt-get install whois**

Whois sorgulama siteleri:

domaintools.com
who.is

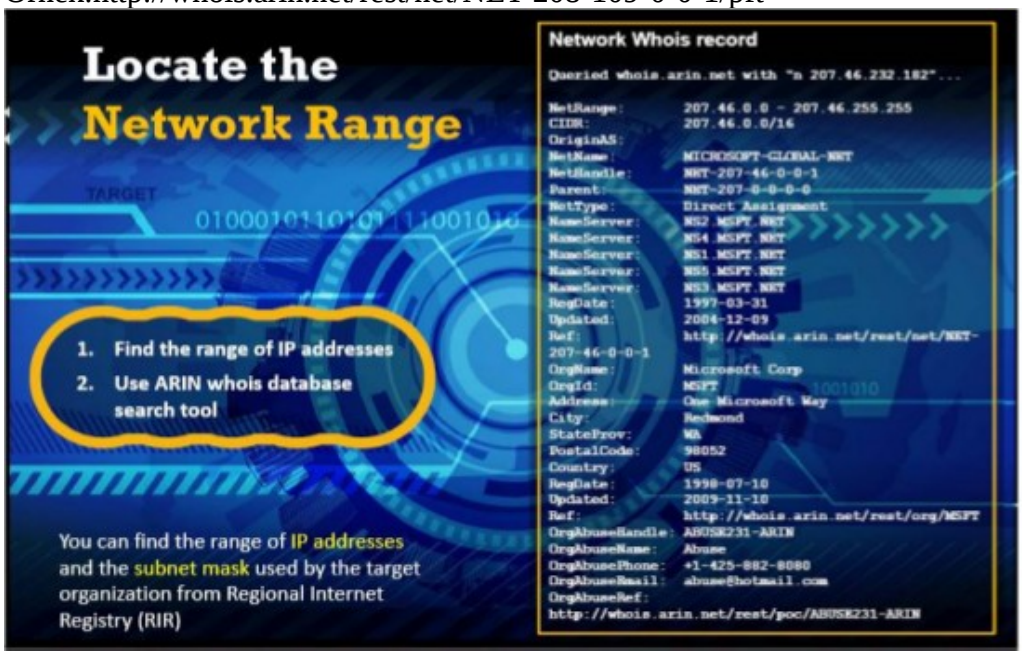
Bölgesel alanadı ve ip sorgulama hizmetleri:

Adres:https://www.arin.net/knowledge/rirs.html



Hedef ip adresinin Ağ subnet aralığını çıkartma:

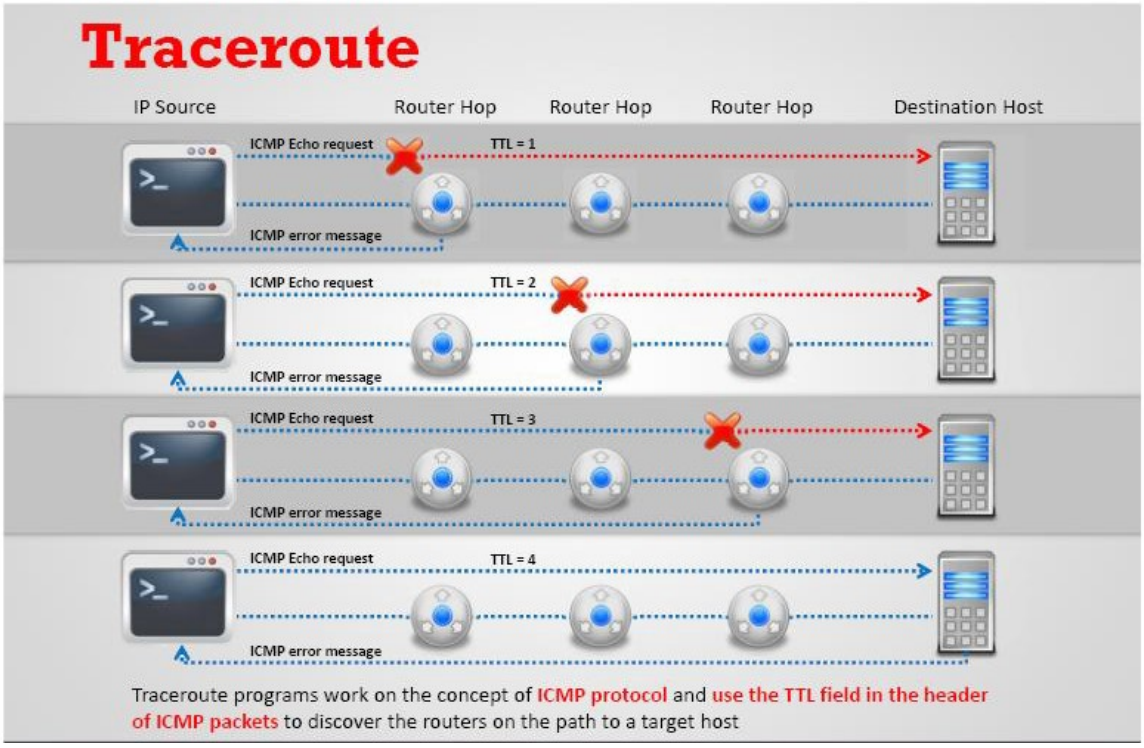
Örnek:http://whois.arin.net/rest/net/NET-208-109-0-0-1/pft



Traceroute:

Traceroute IP başlığındaki TTL (time-to-live) alanını ve ICMP protokolünü kullanır.

TTL, IP başlığında 8 bitlik alana sahiptir. İlk değeri gönderen tarafından atanır ve bu değer , üzerinden geçtiği her hopta router tarafından azaltılır. TTL alanının amacı sonsuz yönlendirme olmasını engellemektir. Bir yönlendirici TTL alanı 0 ya da 1 olan bir veri paketi almış ise paketi başka bir yere yönlendirmez ve kaynak hostuna ICMP "zaman aşımı" mesajı gönderir. ICMP mesajına sahip olan veri paketi router'ın ip adresini kaynak adresi olarak alır. Traceroute bu sistemi kullanır.Traceroute hedef hosta TTL alan değeri 1 olan veri paketi gönderir. Veri paketini alan router, TTL değerini düşüremediği için hedefe giden yoldaki diğer router'a yönlendirme yapmaz ve geriye icmp "zaman aşımı" mesajını gönderir. Böylece ilk yönlendiricinin IP adresini bulur. Traceroute diğer adımda hedef hosta TTL değeri 2 olan veri paketi gönderir ve yoldaki ikinci router'ın IP adresini bulur. Bu yolla hedef hosta ulaşılıncaya kadarki yönlendiriciler tanımlanır.



Traceroute komutuyla hackerlar hedefin ağ topolojisi çıkartabilir gönderilen paketin geçtiği yolları tespit edebilir,firewall cihazlarını tespit edebilir

Online Görsel Traceroute web sitesi:

http://traceroute.monitis.com/

Örnek:

Linux terminalinde :traceroute komutu kullanılmalıdır.

Windows'da ise cmd.exe üzerinde tracert komutu kullanılmalıdır.

Örnek:

linux örnek:traceroute deneme.com
windows örnek:tracert deneme.com

DNS TOOLS:

DNS Data Extraction Siteleri:

http://network-tools.com
http://intodns.com/

DNS bilgisi toplama ARAÇLARI:

NSLOOKUP:

İsim sunucularını interaktif olarak sorgulamamızı sağlayan araç.

Windows ve linux'da da kullanılabilen aktif bilgi toplama aracı.

Basit Kullanımı:

cmd.exe açıldıktan sonra sırasıyla

Windows için komutları verildiği takdir de:
nslookup.exe

set type=any

deneme.com

dns bilgisi dökülmektedir.

help yazarak diğer komutların listeside görülebilir.

DİG:

dig aracı ile dns ile ilgili aktif bilgi toplama gerçekleştirilir.

Komut adımları sırasıyla:

dig sahibinden.com

dig NS sahibinden.com

dns01.sahibinden.com adresi recursive sorgulara cevap vermektedir.Bu dns poisoning saldırılarının gerçekleştirilmesine olanak sağlar!

dig deneme.com @dns01.sahibinden.com

Aynı işlemi pasif olarak detaylı olarak raporlayan ve bilgi veren web sitesi görülebilir:

“http://www.dnsstuff.com/tools#dnsReport|type=domain&&value=sahibinden.com”

DNS Data Extraction Siteleri:

http://network-tools.com
http://intodns.com/
http://www.dnsstuff.com/

PENTEST-TOOLS:

Alan adı ile ilgili isim sağlayıcı bilgilerini verir.Zone transfer yapmak mümkündür.Alt alan adlarını mail sunucu bilgilerini dns kayıtlarını sorgulamak mümkündür.

Adres:https://pentest-tools.com/reconnaissance/dns-search-online

Aynı işlemi dig ile şu şekilde yapmak mümkündür:

dig AXFR example.com @ns1.exampledns.com.

GOOGLE HACKING:

Google Hacking Database:

Adres:http://www.exploit-db.com/google-dorks/

Google arama operatörleri için:

Bütün arama operatörleri aşağıdaki adreste yer almaktadır:

http://www.googleguide.com/using_advanced_operators.html

Google arama ipuçları:

intitle index of "parent directory"

Sayfa başlığında "yönetim" paneli olan siteleri listeler
allintitle:yönetim

Web sayfalarındaki alt klasörleri, urlleri arar.
inurl:

Web sitesinin altındaki bütün herşeyi arar:

site:sahibinden.com/*.php: **Web sitesinde yer alan bütün php dosyalarını listeler**
site:*.sahibinden.com: **Web sitesindeki bütün herşeyi listeler.**

Web sitelerindeki dosya uzantılarına göre arama yapar.
filetype:pdf : **Örnek olarak pdf dosyalarını verdim.**

Kullanılabilecek hazır araçlar:

Goolag Scanner

Adres:www.soldierx.com
Açık sistemleri ve dışarıya açık ağlardaki açıklıkları aramak için kullanılan arama motoru: Shodan

Site kapanmış bile olsa arşiv bilgisini bulmak mümkündür.
Archive.org bilgi toplama araçları içerisinde en sık kullanılan web sitesidir.Crawl ettiği web sitelerinin geçmiş bilgilerini saklayarak yıllar öncesindeki bilgilere bile ulaşılabilmektedir.
Websitewatcher tool:site sayfa kayıt tarihi çekme

Dirbuster nedir?

Dirbuster web sitesine deneme yanılma yöntemi dahil olmak üzere wordlist ekleyerek de bütün urlleri listeler.

Bütün araçları barındıran online footprinting websitesi :
www.dirk-loss.de/onlinetools.htm

Otomatize bilgi toplama aracı Harvester:

Adres:https://code.google.com/p/theharvester/

Kali işletim sisteminde mevcuttur.

Eposta ile ilgili bilgi toplama:

Gelen epostaların kaynağını görüntüleyerek detaylı bilgi edinilebilir.

Eposta maillistelerine üye olunarak bilgi toplamak mümkündür.

Email Tracker Pro:www.emailtrackerpro.com

Eposta bildirim ve bilgi takibi:

http://www.readnotify.com/

http://www.getnotify.com/

Ücretli eposta bildirim ve bilgi takibi:

http://www.didtheyreadit.com/

Faydalanılabilecek Kaynaklar:

http://www.slideshare.net/leminhvuong/module-2-foot-printing
http://ptgmedia.pearsoncmg.com/images/9780789735317/samplechapter/0789735318_CH03.pdf