MEB - Öğretmen Yetiştirme ve Geliştirme Genel Müdürlüğü Siber Güvenliğe Giriş Eğitimi 2.DERS 07.04.2020

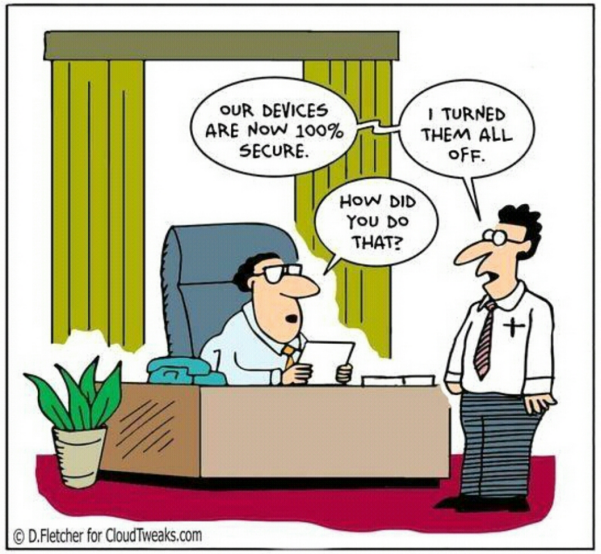
Introduction to Cybersecurity v2.1

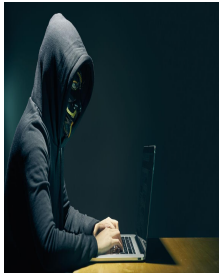
01.04.2020 – Bölüm 1: Siber Güvenlik Gereksinimi
1.Ders Öğrendiklerimiz! Farkındalıklarımız!

Çevrimdışı Kimlik

Çevrimiçi Kimlik

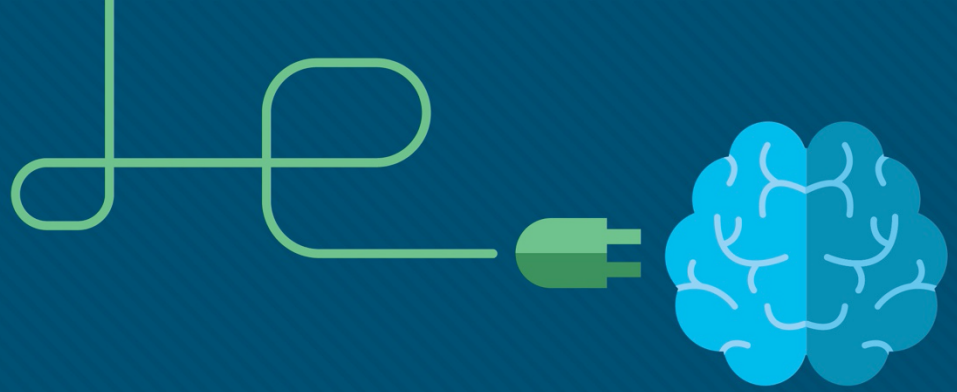
KVKK





Siber sadece Internet DEĞİLDİR, çok daha fazlasıdır.

Bölüm 2: Saldırılar, Kavramlar ve Teknikler



Introduction to Cybersecurity v2.1

Bölüm 2 – Öğreneceklerimiz!
Bölümler ve Hedefler

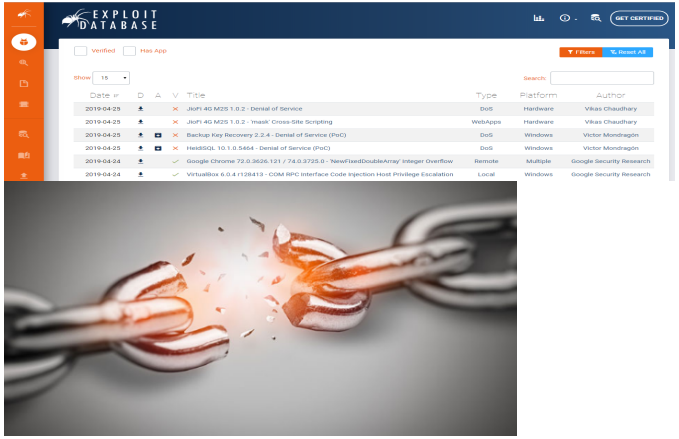
- 2.1 Bir Siber Saldırıyı Analiz Etme
  - Bir siber saldırının özelliklerini ve işleyişini açıklayın.
    - Bir güvenlik açığından nasıl yararlandığını açıklayın.
    - Güvenlik açıklarına ilişkin örnekleri belirleyin.
    - Kötü amaçlı yazılım türlerini (Malware Types) ve semptomlarını açıklayın.
    - Sızma yöntemlerini açıklayın.
    - Hizmeti engelleme (DoS) için kullanılan yöntemleri açıklayın.
- 2.2 Siber Güvenlik Ortamı
  - Siber tehdit ortamındaki trendleri açıklayın
    - Karma saldırıyı (blended attack) tanımlayın.
    - Etki azaltmanın (impact reduction) önemini açıklayın.

2.1 Bir Siber Saldırıyı Analiz Etme

Güvenlik Açıklarını Bulma

https://www.securityfocus.com/

- ***İstismar (exploit)***, bilinen bir güvenlik açığından !ZAFİYET! yararlanmak için yazılmış bir program.
- ***Saldırı (attack)*** , bir güvenlik açığına karşı bir istismar (exploit) kullanma eylemidir.
- Yazılım güvenlik açığı (Software vulnerability)
  - İşletim sistemindeki veya uygulama kodundaki hatalar
  - **SYNful Knock** – Cisco IOS'ta Güvenlik Açığı
    - saldırganların yönlendiricileri kontrol etmesini sağlar
    - ağ iletişimini izler
    - diğer ağ aygıtlarına bulaşabilir
  - **Project Zero** – Google, yazılım açıklarını bulmaya adanmış kalıcı bir ekip oluşturdu..



Bir zincir ancak en zayıf halkası kadar güçlüdür!

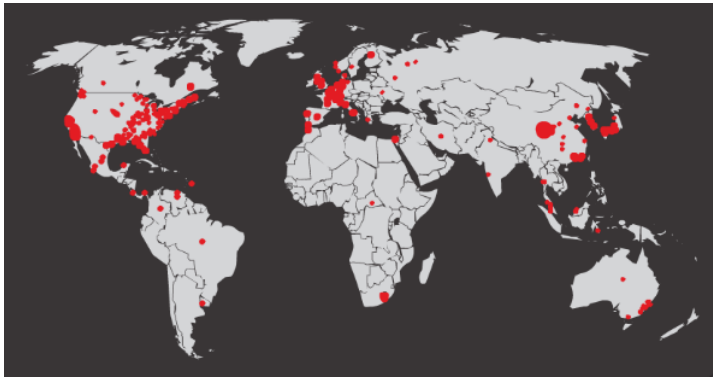
- Donanım güvenlik açığı (Hardware vulnerability)
  - Donanım tasarım kusurları
  - **Rowhammer** - RAM bellek istismarı, verilerin yakındaki adres bellek hücrelerinden alınmasına izin verir.

Güvenlik Açıklarını Sınıflandırma

- **Buffer Overflow (Arabellek Taşması)**
  - Veriler bir arabellek sınırlarının ötesinde yazılır
- **Non-validated Input (Kont rol Edilmemiş Giriş)**
  - Programları istenmeyen bir şekilde davranmaya zorlama
- Race Conditions (Yarış koşulları)
  - Yanlış sıralanmış veya zamanlanmış etkinlikler
- Güvenlik Uygulamalarındaki Zayıf Yönler
  - Kimlik doğrulama (authentication), yetkilendirme (authorization) ve şifreleme (encryption) yoluyla hassas verileri koruyun
- **Erişim Kontrol Sorunları**
  - Fiziksel ekipman ve kaynaklara erişim kontrolü
  - Güvenlik uygulamaları

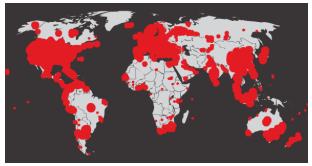
Kötü Amaçlı Yazılım Türleri

- Kötü amaçlı yazılım (Malware), verileri çalmak, erişim denetimlerini atlamak, sisteme zarar vermek veya bir sistemin güvenliğini aşmak için kullanılır.
- **Kötü Amaçlı Yazılım Türleri (Malware Types)**
  - **Spyware** - kullanıcıyı takip et ve gözetle
  - **Adware** - reklam yayınlama, genellikle casus yazılımlar ile gelir
  - **Bot** - otomatik olarak eylem gerçekleştir
  - **Ransomware** (Fidye Yazılımı) - bir ödeme yapılıncaya kadar ; bir bilgisayar sistemini veya verileri esir tutmak
  - **Scareware** (Kortkutma Yazılımı)- kullanıcıyı korkuya dayalı belirli bir işlem yapmaya ikna etme.



Initial Code Red Worm Infection

Kötü Amaçlı Yazılım Türleri (devamı)



Code Red Worm Infection
19 Hours Later

- Kötü Amaçlı Yazılım Türleri (Cont.)
  - **Rootkit** - arka kapı oluşturmak için işletim sistemi derinliklerine yerleşen zararlı yazılımlar.
  - **Virus** (Virüs)- diğer çalıştırılabilir dosyalara eklenen kötü amaçlı çalıştırılabilir kodlar.
  - **Trojan horse** (Truva Atı)- istenen bir operasyon kılıfı altında kötü amaçlı operasyonlar gerçekleştirir.
  - **Worm** (Solucan)- ağlardaki güvenlik açıklarından yararlanarak bağımsız olarak kendilerini çoğaltırlar.
  - **Man-in-the-Middle** (Aradaki Adam) kullanıcının bilgisi olmadan bir cihaz üzerinde kontrol sahibi olun!
  - Saldırgan iki taraf arasındaki trafik için arada veriyi okur ve değiştirir, iletişimin ortasına konumlanır. En popüler olanı hedef kullanıcı ağ trafiğini yakalamak için saldırganın erişim noktası olarak hareket eden bir laptop olmasıdır. Genellikle güvenliksiz halka açık ağlarda yapılır.
  - **Man-in-the-Mobile** – (sms dogrulamali internet bankaciligina musallat olmus atak cesidi. hedef cep telefonlarina (symbian ve blackberry) bulastirilarak gelen sms kodu saldirgan kisiye yonlendirilir)

Kötü Amaçlı Yazılımın Belirtileri

- CPU kullanımında artış var.
- Bilgisayar hızında bir azalma var.
- Bilgisayar sık sık donuyor veya çöküyor.
- Web'de gezinme hızında bir azalma var.
- Ağ bağlantılarında açıklanamayan sorunlar var.
- Dosyalar değiştirilmiş.
- Dosyalar silinmiş.
- Bilinmeyen dosyalar, programlar veya masaüstü simgeleri var.
- Çalışan bilinmeyen prosesler var.
- Programlar kapanıyor veya kendilerini yeniden yapılandırıyorlar
- E-posta, kullanıcının bilgisi veya rızası olmadan gönderiliyor.

Sosyal Mühendislik (Social Engineering)

- Sosyal Mühendislik – eylem yapmak üzere farklı kişi gibi gözükme veya gizli bilglerin ele geçirilmesi
  - **Pretexting** (Sahte Senaryolar Uydurmak)- bir saldırgan bir kişiyi arar ve ayrıcalıklı verilere erişim elde etmek amacıyla onlara yalan söyler.
  - **Tailgating** (Çok Yakın Gitmek)- girmenin izne tabi olduğu bir yere yetkisiz bir kişinin (saldırganın) yetkili bir kişinin arkasına kuyruk misali eklenerek girmeye çalışmasına denir.
  - **Something for something** **(**Bir şey için bir şey) **(Quid pro quo)** - bir saldırgan bir şey karşılığında diğer taraftan kişisel bilgi ister. (**if you don't pay the product, you are the product!)**

Wi-Fi Şifre Kırma

- Wi-Fi Şifre Kırma – Şifreleri ortaya çıkarma
  - **Sosyal Mühendislik** - Saldırgan, parolayı bilen bir kişiden parolayı elde etmeye çalışır.
  - **Kaba kuvvet saldırıları (Brute-force attacks)** - Saldırgan, şifreyi tahmin etmek için birkaç olası şifreyi dener.
  - **Teknoloji Açıkları** – WPS Açıkları – WPA2 Crack Açığı. **ÇÖZÜM! GÜNCEL YAZILIM!!!**

Brute Force nedir?

Türkçesi Kaba Kuvvet ve zorlamak anlamlarına gelir. Brute force, bir sistem şifresini deneme yanılma yoluyla ele geçirmeye çalışmaktır. Bunun için bazı araçlar yapılandırılmış ve kullanılmaktadır.

Örnek bazı brute forcing araçları şunlardır:

- Hydra
- Medusa
- John the Ripper
- OphCrack
- Ncrack
- Aircrack-ng
- Rainbow Crack
- Cain and Abel
- Hashcat

Phishing (Oltalama/Yemleme)

- **Phishing** (Oltalama)
  - kötü niyetli taraf meşru ve güvenilir bir kaynaktan geldiği düşünülen sahte bir e-posta gönderir
  - alıcıyı cihazlarına kötü amaçlı yazılım yüklemeye veya kişisel veya finansal bilgileri paylaşmaya yönlendirmek
- **Spear phishing** (Hedef Odaklı Oltalama)
  - hedefi iyi belirlenmiş bir oltalama saldırısı

Günümüzde MALWARE trendleri

2014 – CRYPTOLOCKER SALDIRISI

Günümüzde MALWARE trendleri

8775563743 nolu hattınıza ait ARALIK-2014 Dönemi Türk Telekom Faturanız

Türk Telekom e-Fatura <haber@eturktelekom.org>

Tarih: 17.12.2014 Çar 15:10

Kime:

TÜRK TELEKOM

E-FATURA (ELEKTRONIK FATURA)

Sayin Müsterimiz,

Son ödeme tarihi **18/12/2014** olan **219,23 TL** tutarindaki güncel faturaniza buradan ulasabilirsiniz.

E-FATURA GÖRÜNTÜLE | E-FATURA ÖDEME

Kağıt tüketimini azaltmak ve çevreyi korumak için e-fatura kullanımı büyük önem taşıyor. Sizde e-fatura tercih ettiginiz için tesekkür ederiz.

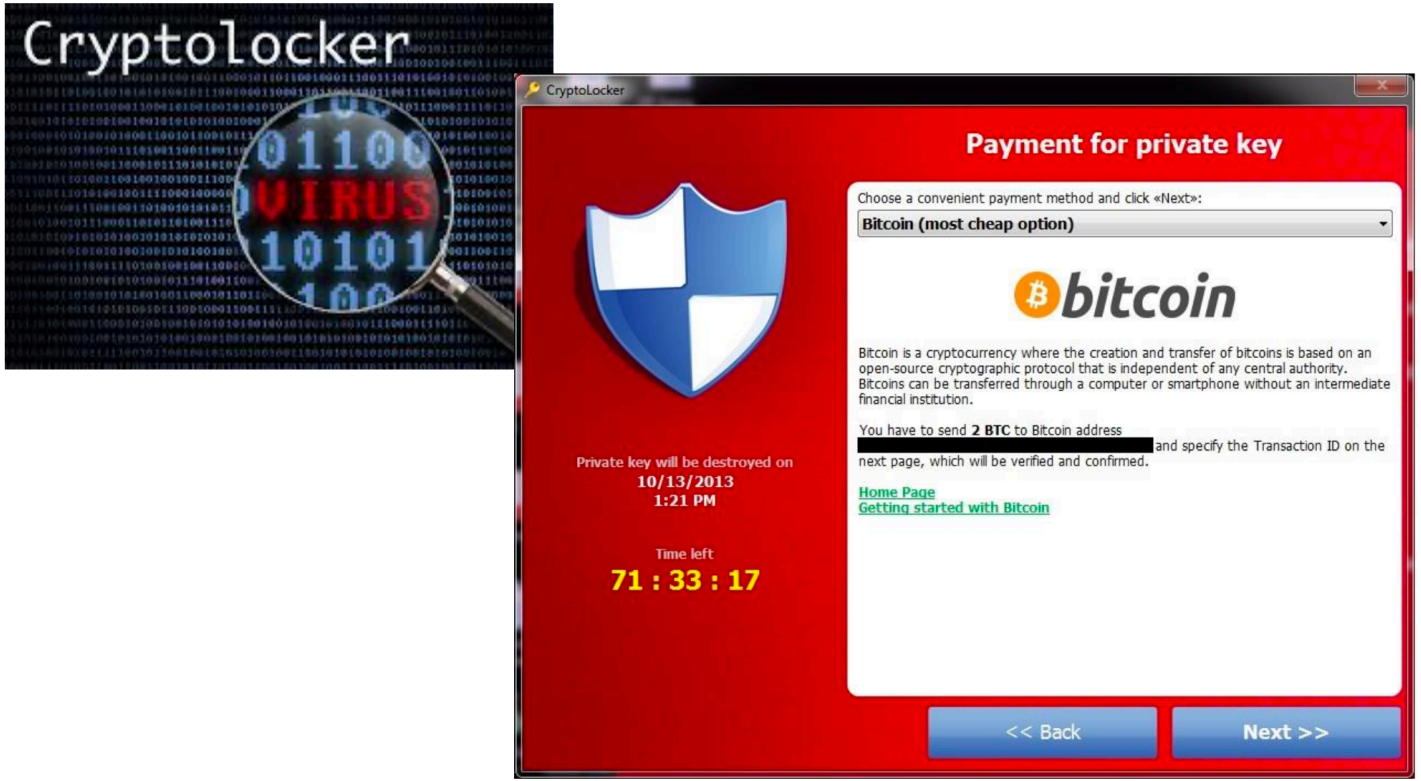
2014 – CRYPTOLOCKER SALDIRISI

Günümüzde MALWARE trendleri

Ad	Değiştirme tarihi
0D01 068.JPG.encrypted	24.03.2015 10:55
0D01 069.JPG.encrypted	24.03.2015 10:55
0D01 071.JPG.encrypted	24.03.2015 10:55
0D01 072.JPG.encrypted	24.03.2015 10:55
0D01 073.JPG.encrypted	24.03.2015 10:55
0D01 074.JPG.encrypted	24.03.2015 10:55
0D01 075.JPG.encrypted	24.03.2015 10:55
0R.70.57-000060.00.jpg.encrypted	24.03.2015 10:55
0R.72.57-000000.00.jpg.encrypted	24.03.2015 10:55
0R.74.00-000000.00.JPG.encrypted	24.03.2015 10:55
001.29.jpg.encrypted	24.03.2015 10:54
1YTU140025T5509.JPG.encrypted	24.03.2015 10:57
02.101.013.JPG.encrypted	24.03.2015 10:54
02.980.021.JPG.encrypted	24.03.2015 10:54
2TU012510-0205.JPG.encrypted	24.03.2015 10:58
2TU012550-0081.jpg.encrypted	24.03.2015 10:58
2TU012610-0067.jpg.encrypted	24.03.2015 10:58
2TU012610-0078.JPG.encrypted	24.03.2015 10:58

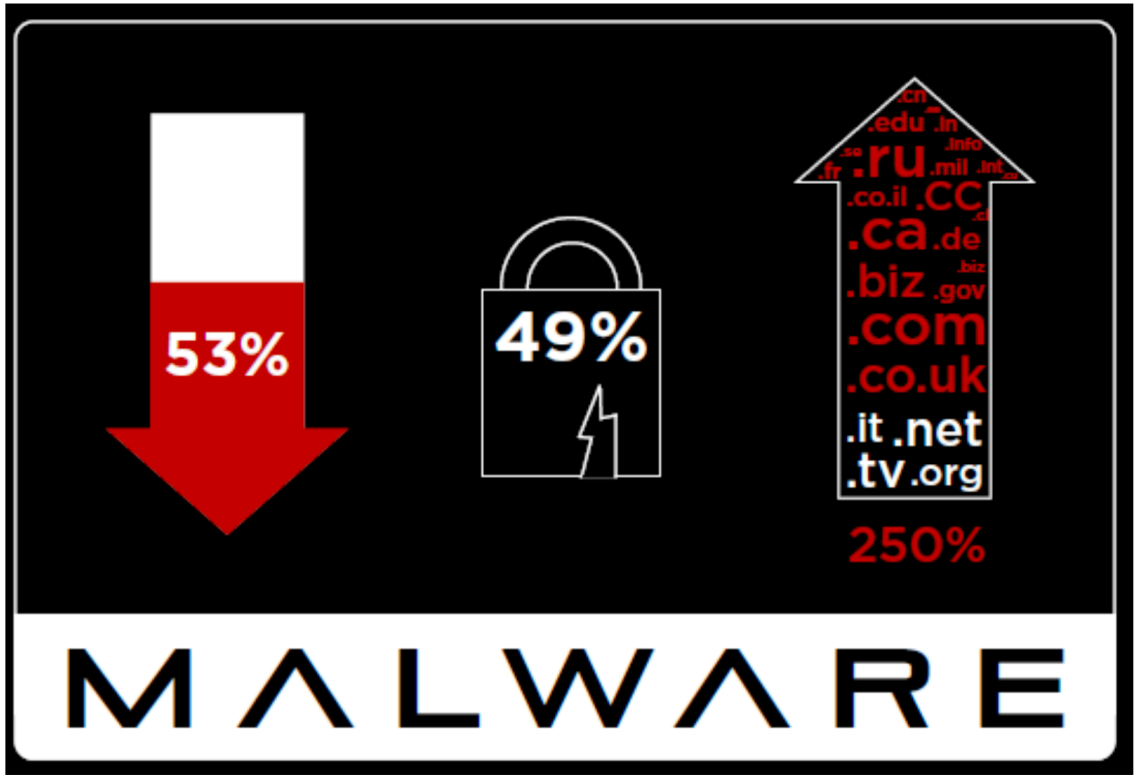
2014 – CRYPTOLOCKER SALDIRISI

Günümüzde MALWARE trendleri



2014 – CRYPTOLOCKER SALDIRISI

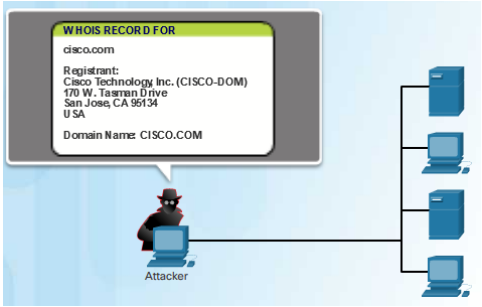
Günümüzde MALWARE trendleri

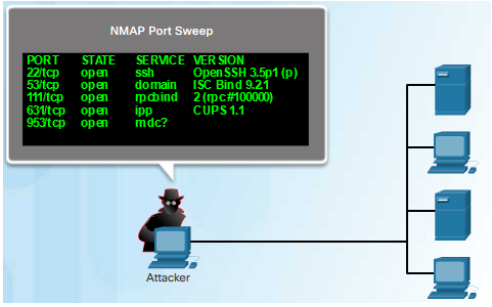


Her gün ortalama 2 farklı tip Malware ortaya çıkıyor.
Güvenlik Açıklarının sadece %49'u için Zararlı Yazılım'lar geliştirilmiş.

Güvenlik Açığı Sömürüsü (Vulnerability Exploitation)

- **Güvenlik Açığı Sömürüsü** – istismar edilecek güvenlik açığı bulmak için tarayın
  - **Adım 1** - Port tarayıcı veya sosyal mühendislik kullanarak hedef sistem hakkında bilgi toplama
  - **Adım 2** - Adım 1'den öğrenilen bilgileri belirleme
  - **Adım 3** - Güvenlik açığı arama
  - **Adım 4** - Bilinen bir istismarı (exploit) kullanma veya yeni bir istismar yazma
- **Gelişmiş Kalıcı Tehdit (Advanced Persistent Threat – APT)** – belirli bir hedefe karşı çok aşamalı, uzun vadeli, gizli ve gelişmiş bir operasyon
  - genellikle iyi finanse edilir
  - özelleştirilmiş kötü amaçlı yazılım yayma





Saldırı Tipleri

- **KEŞİF ATAKLARI** (Reconnaissance Attacks)
- **ERİŞİM ATAKLARI** (Access Attacks)
- **SERİVS DIŞI BIRAKMA ATAKLARI** (Denial of Services DOS)

KEŞİF ATAKLARI (Reconnaissance Attacks)

- Özellikle saldırı öncesi bilgi toplamak için yapılan saldırıdır. Bir keşif saldırısında kötü niyetli saldırgan genellikle ip adreslerinin etkinliği için hedef ağa ping sweep (ping tarama) yapar. Daha sonra NMAP gibi program kullanarak port taramaları yaparak servisleri keşfeder. Elde edilen bilgilerden ana bilgisayara saldırı yapar. Hedefin İşletim Sistemi türü sürümü için bağlantı noktalarını sorgular. Açıklıkları tespit ederek sistemi sınar.
- www.ripe.net
- **Keşif Saldırıları için kullanılan araçlar**
- Packet Sniffers (Paket dinleyici) Wireshark
- Ping Sweeps (ping tarayıcı) NMAP
- Port scans (port tarayıcı) NMAP
- İnternet information Queries WHOIS

Keşif Saldırıları için kullanılan araçlar

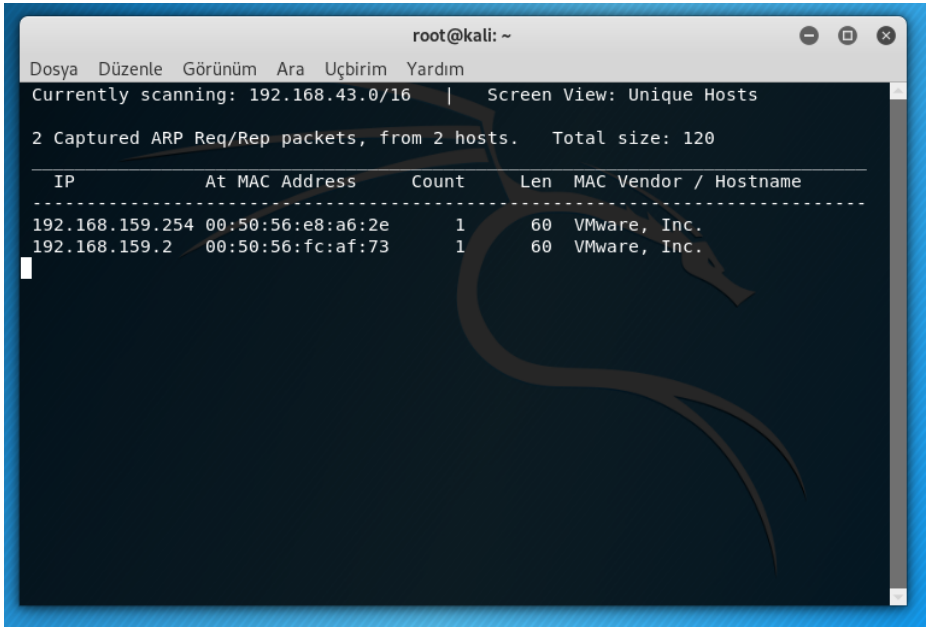
- Parmak İzi Araştırması - Hedef hakkında bilgi toplama
- Ortak Bilgi Kaynakları ve Araçları - Kurumsal web sitesi - Sosyal Mühendislik - Google Hacking - DNS -whois, nslookup
- Hızlı Demo -Google Hacking Google‟da anahtar kelimeleri arayın: «people.lst» veya «passwd» veya «htaccess» vs.

Nmap

- Nmap :En yaygın olarak kullanılan port tarayıcı programıdır. Nmap, açık kaynak kodlu bir yazılım olup ücretsizdir. Hem Windows hem de Linux üzerinde çalışabilmektedir. Nmap programının en önemli özellikleri şunlardır:
  - TCP ve UDP port taraması yapabilmektedir.
  - İşletim sistemi tespiti yapabilmektedir.
  - Çalışan servisleri tespit edebilmektedir.
  - Yazılımların sürümünü tahmin edebilmektedir.
  - Bir ağdaki canlı bilgisayarları tespit edebilmektedir.
  - Raporlama yeteneği bulunmaktadır.

- Test sonucunda HTML formatında raporlar çıkarmaktadır. Nmap, komut satırıyla çalışan bir programdır. Ancak, Zenmap isminde kullanıcı ara yüzüne sahip olan sürümü de çıkmıştır.

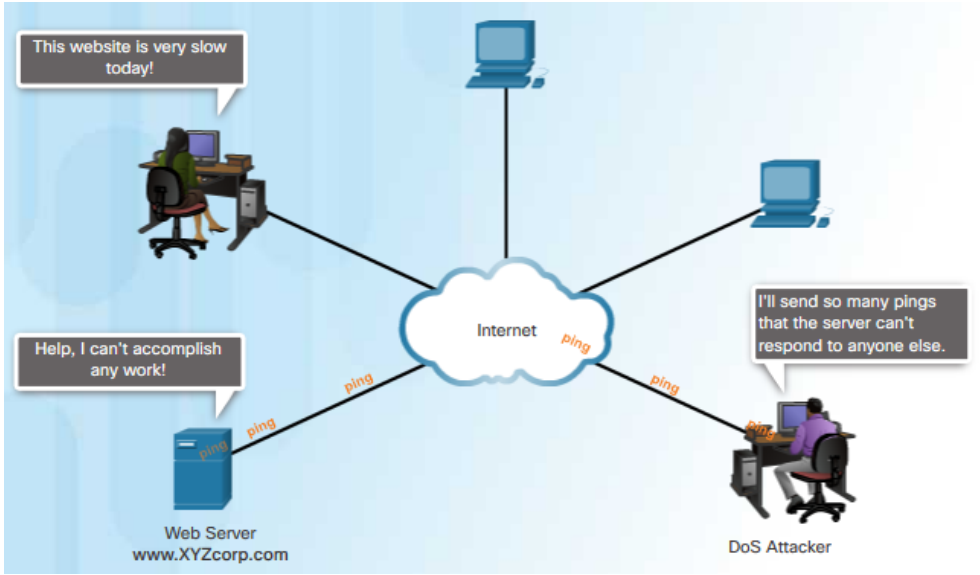
Netdiscover



Kali terminalden netdiscover yazmak tüm ağı taramak için yeterlidir.

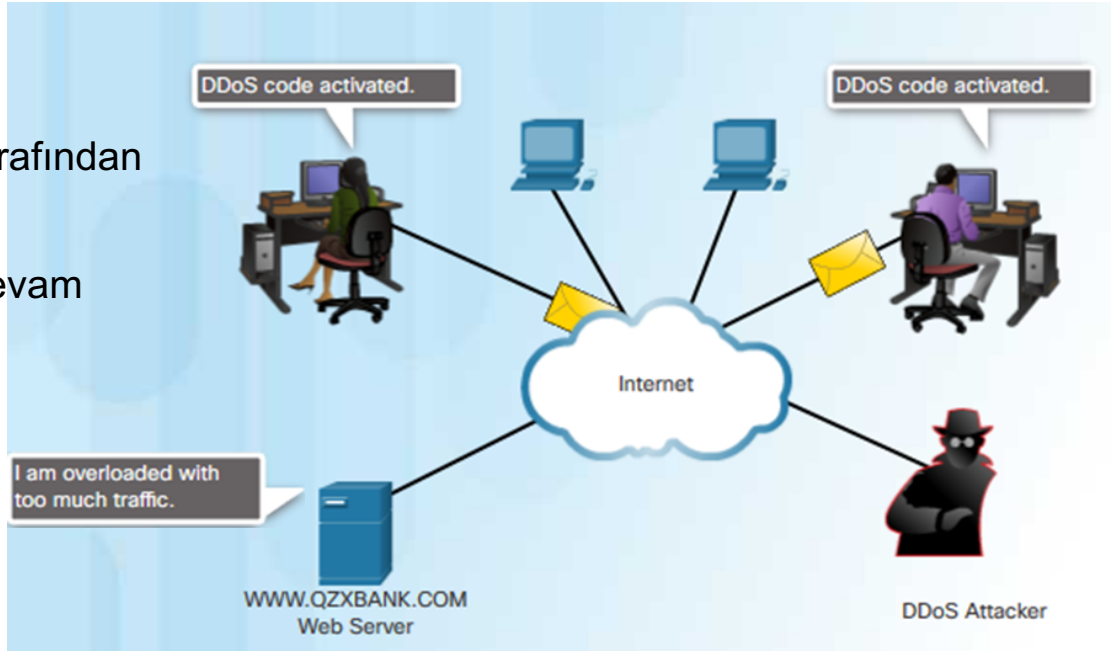
DoS (Denial of Service)

- DoS, ağ hizmetlerinin bozulmasıdır
  - **Çok yoğun bir trafik akışı**- bir ağa, ana bilgisayara veya uygulamaya, işleyemediği oranda çok büyük miktarda veri gönderilir
  - **Kötü amaçlı biçimlendirilmiş paketler**- kötü amaçlı biçimlendirilmiş paket bir ana bilgisayara veya uygulamaya gönderilir ve alıcı bu paketi işleyemez



DDoS (Distributed Denial of Service)

- DoS'a benzer, birden çok koordineli dağıtık kaynaktan gelen saldırılardan oluşur
- Botnet - enfekte olmuş bilgisayar ağı
- Zombie - enfekte olmuş bilgisayar
- Zombiler merkezi işleyici sistemleri tarafından kontrol edilir.
- Zombiler, bilgisayarlara bulaşmaya devam ederek daha fazla zombi yaratıyorlar.



SEO Zehirlemesi

- SEO (Search Engine Optimization)
  - Arama Motoru Optimizasyonu
  - Bir arama motorunun bir web sitesinin sıralamasını iyileştirme teknikleri
- SEO Zehirlemesi
  - Kötü amaçlı web sitelerine gelen trafiği arttırır
  - Kötü amaçlı siteleri daha yüksek sıralamaya zorlar

2.2 Siber Güvenlik Ortamı

Karma Saldırı nedir?

- Bir hedefi açığa çıkarmak (compromise) için birden fazla teknik kullanır.
- Solucanlar, Truva atları, casus yazılımlar, tuş kaydediciler, spam ve oltalama (phishing) düzenlerinden oluşan karma yöntemler kullanır.
- Ortak karma saldırı örneği
  - Spam e-posta mesajları, anlık mesajlar veya bağlantıları dağıtmak için yasal web siteleri
  - Oltalama (phishing) e-postalarıyla birlikte DDoS
- Örnekler: Nimda, CodeRed, BugBear, Klez, Slammer, Zeus/LICAT, and Conficker

Etki Azaltma Nedir?

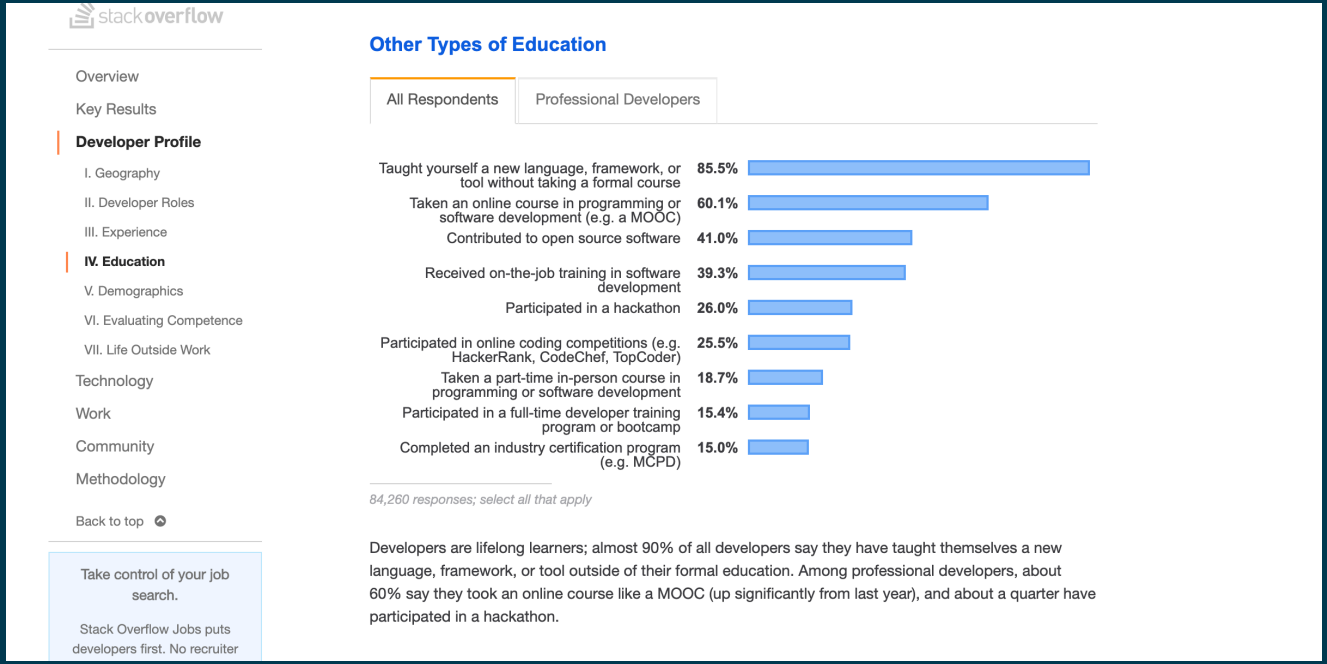
- Sorunu iletin
- Samimi ve hesap verebilir olun
- Detayları sağlamak
- İhlalin nedenini anlayın
- Gelecekte benzer bir ihlali önlemek için adımlar atın
- Tüm sistemlerin temiz olduğundan emin olun
- Çalışanları, ortakları ve müşterileri eğitin

2.3 Bölüm Özeti

Özet

- Güvenlik açıklarına ilişkin örnekleri inceleyin.
- Bir güvenlik açığından nasıl faydalanıldığını açıklayın.
- Kötü amaçlı yazılım türlerini ve belirtilerini, sızma yöntemlerini, hizmet engelleme için kullanılan yöntemleri açıklayın.
- Bir karma saldırıyı (blended attack) ve etki azaltmanın önemini açıklayın.

SORU ve CEVAP!



https://insights.stackoverflow.com/survey/2019#developer-profile

TEŞEKKÜRLER
Arzu KİLİTCİ CALAYIR
www.arzukilitci.com

Kaynak : Cisco Ağ Akademisi
(https://www.netacad.com/portal/teaching)
Kaynak - Çeviri: Ağ Yöneticileri Derneği
(http://www.agyoneticileri.org/)

07.04.2020