Necmettin Erbakan Üniversitesi

Bilgi Güvenliği
2022-2023 Güz Dönemi

Dr. Alperen Eroğlu
aeroglu@erbakan.edu.tr

Hafta-9

Kötü Amaçlı Yazılımlar, Siber Tehditler ve Saldırılar (DDOS Ataklar vb.) ve Analizi

https://enterprise.comodo.com/what-is-malware-software.php

https://www.accesssystems.com/blog/4-faces-of-malware-the-difference-between-viruses-trojans-spyware-ransomware

Hafta-9

- Zararlı yazılım (**malware**) bilişim sistem ve cihazlarına zaralı olan her türlü kötü amaçlı program ve kodu tanımlamak için kullanılır.

Hafta-9

Bazı zararlı yazılım (malware) şu şekildedir:

- Virüsler
- Solucanlar (Worms - Kurtçuklar)
- Truva Atları (Trojans)
- Casus Yazılımlar (Spyware)
  - Parola Çalıcılar
  - Bankacılık Truva Atları
  - Emotet
  - Bilgi çalıcılar (Infostealers)
  - Tuş kaydediciler (Keyloggers)
- Rootkit
- Fidye Yazılımları (Ransomware)
- Uzaktan Yönetim Aracı (RAT)
- Cryptojacking
- İstismar Kitleri (Exploit Kit-EK)
- Java Tabanlı İstismarlar
- iFRame İstismarı
- Water Holing
- Zero-Day

Hafta-9

Virüsler

- İnsan etkileşimine ihtiyaç duyarlar.
- Bir dosyanın açılmasıyla, bir e-postanın okunmasıyla, bir sistem ön yüklemesiyle veya bir programın çalıştırılmasıyla yayılır.
- Bilişim sistemlerinin normal çalışmasını etkilerler ve bir bilgisayardan bir diğerine yayılmak için tasarlanırlar,
- Virüsün aktif olarak çalışması için saklandığı programın çalıştırılması ya da ilgili dosyanın açılması gereklidir.
    - Boot virüsleri (her açılışta kontrolü ele geçiren)
    - Web scripting virüsleri (açıkları istimar eder)
    - Browser Hijacker (Web tarayıcısının fonksiyonlarını ele geçirerek otomatik yönlendirme yapar)
    - Resident Virüsler (Yerleşik), Aksiyon virüsleri (Bir dosya açıldığında)
    - Polymorphic Virüsler (Her dosya çalıştırıldığında kodunu değiştiren)
    - Bulaşan virüsler (Sistem fonksiyonlarına yerleşik virüsler)
    - Makro Virüsler (e-mail eklentileri bulaşır)

Hafta-9

Solucanlar (Worms)

- İnsan etkileşimine veya başka bir çalıştırılabilir dosya ya da programa ihtiyaç duymazlar.
- Hedef sistemdeki açıklardan faydalanarak veya sosyal mühendislik yöntemleriyle yayılırlar.
- E-mail eklentisi olarak gönderilen bir solucan dosya açıldığında sizi zararlı bir web sayfasına yönlendirerek bilgisayara otomatik olarak indirilmesi ile bulaşabilir.
- İndikten sonra kendi kendine çalışarak kendini kopyalar ve bant genişliği ve sistem kapasitesini etkileyerek sistemi çalışmaz hale getirebilir.
- Bazı türler dosyaları değiştirebilir, silebilir ya da backdoor açarak saldırganlar için sisteminizi açık hale getirebilir.
- Örnek: 2010 yılında Temmuz ayında Stuxnet isimli bilgisayar solucanı İran'ın nükleer silah üretimini sabote etmek amacıyla tarihte ilk defa siber silah olarak kullanılmıştır.

Hafta-9

Truva Atları (Trojans)

- Truva atları faydalı bir yazılım içerisinde sisteme bulaşabilir...
- Eklendikleri program dosyasının çalıştırılması sonucu aktif olurlar ve kullanıcıların kopyalaması ile yayılırlar.
- İzleme, yetkisiz erişim için imkan sağlayabilir, internet hız genişliğinin bir kısmını kullanarak sistemi yavaşlatabilir, bilgi çalabilir, dosya silebilir ya da dosya üzerinde değişiklikler yapabilir.
- Nesnelerin interneti (Internet of Things) sistemlerin yagın olması ile bu cihazların Truva atı olarak kullanılması da artmıştır.
- Yaptıkları eylemlere göre şu şekilde sınıflandırılabilirler:
- Arka kapı (backdoor) : botnet veya zombi bilgisayar oluşturmak için kullanılır.
- İstismar, Rootkit, Banker, DDOS, indirici, damlalık (dropper), sahte antivirüs, Trojan-gamethief (Online oyunlarda username, password)
- IM (ICQ, MSN Messenger ve Skype anlık mesajlaşma program. usernam ve passwrod)
- Trojan-SMS, Trojan-Spy, Trojan-Mailfinder, Trojan-ArcBomb, Trojan clickers, Trojan proxy

Hafta-9

Casus Yazılımlar (Spyware)

- Bilgisayarlara veya mobil aygıtlara bulaşarak kullanıcı hakkında internet kullanım alışkanlıkları, e-mail adresleri, kredi kartı bilgileri, parolalar gibi bazı kişisel önemli bilgilerin kullanıcının bilgisi ve onayı dışında elde edilip kötü niyetli kişilere gönderilmesini sağlayan yazılımlardır.
- Bir yazılımın yüklenmesi (eğer güvenilir kaynak değilse) esnasında sisteminize yüklenmesine izin verilmiş olabilir.
- Zararlı yazılımlarda olduğu gibi Truva atları veya istismar kitleri vasıtasıyla bilgisayar veya mobil cihaza bulaşabilir.
- Parola çalıcılar, (Password Stealers), Bankacılık truva atları, emotet, bilgi çalıcılar, tuş kaydediciler çeşitli casus yazılım kategorilerindendir.
- Örneğin 2018 yılında ön plana çıkan bankacılık casus yazılımları: Emotet, Trickbot, Panda Banker (Zeus), URLZone (Bebloh), Ursnif(Gozi), IcedID, GootKit, Dridex, Corebot ve TinyNuke

Hafta-9

Casus Yazılımlar (Spyware) -- EMOTET

- Emotet 2014 yılında ortaya çıkmıştır
- (Mealybug tarafından geliştirilen), polimorfik yapısı sayesinde (imza tabanlı tepiti önlemek için her indirmede kendini değiştiren bir yapıya sahip)
- İlk başta JavaScript tabanlı makro içeren dökumanlar yoluyla sisteme bulaşabilmektekdir
- Her bir olay başına bir milyon dolara varan temizleme maliyetiyle özel sektör, bireyler, hükümetler ve organizasyonlar açısından en zarar verici ve yıkıcı yazılımlar arasında yer almaktadır.
- Windowstaki EternalBlue/DoublePulsar açıklarını kullanırlar.

Okuma Önerisi:
https://www.malwarebytes.com/spyware

Hafta-9

Rootkit

- İşletim sistemi kernel'a (çekirdek) sızarak saldırganlara tam yetki veren zararlı bir yazılımdır.

- Kernel seviyesinde olması tespit, analiz ve silme işlemlerini zorlaştırmaktadır.

- Bu son derece tehlikeli yetki ile, kullandığınz hesaplar, banka ve kredi kartı bilgileri, bilgisayarınızın DDoS veya Botnet amacıyla kullanarak sanal saldırıların yapılması, bilgisayara ya da telefona bağlı aygıtları (kamera, mikrofon gibi) donanımların kontrolüne kadar ilerler.

- 8 farklı tip: Kernel Rootkit, Firmware Rootkit, Application Rootkit, Memory Rootkit (RAM üzerinde), Bootkit Rootkit (Sistem başladığında), Persistent Rootkits (Sistem açık kaldığı sürece), Library rootkits (.dll gibi), Hyperviser Rootkits (VMM) (Heyper-V, VmWare gibi sistemleri hedef alırlar),

Hafta-9

Fidye Yazılımlar - Ransomware

- İşletim sistemine bulaşarak dosyaları kullanılamazz hale getiren, dosyalara erişimi engelleyen ve şifreleyen zararlı yazılımlara verilen genel ad.
- Saldırganlar dosya erişimi için Bitcoin ile ödeme talep ederler.
- Ağ tabanlı ransomware slolucanlarının geliştirilmesi ve ransomware yayılımı için ağ vektörünün kullanılması bu saldırı tipini yaygınlamtırmıştır.
- 2017'de WannaCry isimli bir ransomware kripto solucanı (fidye yazılımı + solucan) yüzden fazla ülkede kişisel ve kurumsal sistemleri etkisi altına almıştır.
- WannaCry ile siber dünyada ilk kez solucan taktikleri ile fidye yazılımı modelinin bir arada kullanılarak gerçekleştirilmesi söz konusu olmuştur.
- WannaCry Windowsta bulunan Server Message Block-SMB EternalBlue daha önceden tanımlanıp kapatılmış olan güvenlik çaığından yola çıkmıştır (Nisan 2017, Shadow Brokers)
- WannarCry temel olarak EternalBlur modüllerini ve DoublePulsar arka kapısını kullanmaktadır.

Hafta-9

Fidye Yazılımlar - Ransomware

- İlk istismar adımı olarak EternalBlue güvenlik açığı kullanılır ve başarılı olunması durumunda DoublePulsar kullanılarak fidye yazılımı yüklenir.
- Fidye yazılımının ne kadar ciddi bir tehlike olduğunun farkında olunması için 516 güvenlik uzmanının katılımıyla gerçekleşen bir anket çalışması dikkat çekici bulgular ortaya koymuştur:
  - En hızlı büyüyen güvenlik tehdidi
  - Katılımcıların %75 i son bir yıılda 5, geri kalanı 6 veya daha çok sayıda fidye saldırısına uğramıştır.
  - Katılımcıların %59 u bu tehdit karşısında savunma açısından özgüvensiz kalmışlar
  - E-mail ve web kullanımı esnasında çalışanlar tarafından zararlı bir etkenin açılması fidye yazılımlarının en çok karşılaşılan bulaşme yöntemidir.
  - %54 phishing e-mail e tepki vermek, %28 i ele geçirilmiş bir web sayfasını ziyeret etmek

https://businessresources.bitdefender.com/ransomware-report-2017

Hafta-9

Fidye Yazılımlar - Ransomware

- %62 finansal veriler
- %61 müşteri bilgileri
- Fidye yazılımı saldırılarının %83 ü uç cihazlar (endpoint) güvenlik araçları ile, %64'ü e-mail ve web ağgeçitleriyle (gateway) ve % 46 sı IDS ile tepit edilmiştir.
- Katılımcıların %77 si en etkili yöntem kullanıcı farkındalığı geliştirmek ve çeşitli eğitimler vermek, %73 ü ise uç cihazlar güvenlik çözümleri, % 72 si ise işletim sistemlerinin yamalarını zamanında yapmak
- Bu tehdide karşılık verirken en etkin çözüm %74 ile veri yedekleme ve yedekten geri yükleme olarak belirtilmiştir. Katılımcıların %96 sının veri yedekleme ve yedekten geri yükleme stratejisi bulunmaktadır.
- Bu saldırıdan sonra %54 ü bir gün içinde, %39 u bir hafta ile beş hafta arasında bir süre ile ancak normal çalışma moduna dönebileceklerini ifade etmektedirler.

https://businessresources.bitdefender.com/ransomware-report-2017

Hafta-9

Fidye Yazılımlar - Ransomware

- Engeller:
  - Savunmaya ayrılan bütçenin azlığı,
  - Bütçe azlığı (ransomware)
  - Son olarak ortaya çıkan ve sürekli güncelllenen istismarların takip edilememesi en önemli engellerden ayrıca;
  - Bütçe açığı (%52), saldırıların artan karmaşıklığı ile mücadele (%42) ve %33 yetersiz insan kaynakları
  - Bu tarz zararlı yazılımlara karşı Windows tabanlı sistemlerin tamamının yamalarının eksiksiz ve zamanında yapılası gerekir. İnternet kanalıyla açık olarak erişiilen SMB'ye sahip işletme ve kurumlar 139 ve 395 numaralı portlardan içeri yönlü gelen trafiği kontrol altında engellemelidir.

https://businessresources.bitdefender.com/ransomware-report-2017

Hafta-9

Uzaktan Yönetim Aracı (RAT) – Remote Administration Tool

- Saldırgana hedef makine çevrim içi olduğu zaman bu makineye sınırsız erişim hakkı veren ve saldırganın bu araçları kullanarak dosya aktarımı, dosya ve programları yönetme (ekleme ve silme), fare ve klavyeyi kontrol altına alma, çeşitli yanıltıcı sistem mesajları gönderme ve cihazın açılıp kapanması gibi faaliyetleri yapmasına izin vermesidir.

- Normalde RAT sistem yöneticilerinin uzaktan sistemleri yönetebildiği fayalı bir sistemken bir saldırganın ele geçirmesi ile tehlikeli bir yönetim aracı haline gelmektedir.

https://www.mcafee.com/blogs/privacy-identity-protection/what-is-rat/#:~:text=A%20RAT%20or%20remote%20administration,turn%20on%2Foff%20your%20device.

Hafta-9

Cryptojacking – (Mining)

- Bir bilgisayarda veya mobil cihazda saklanan ve ilgili makinenin kaynaklarını örneğin işlemci gücü kullnarak kriptopara birimleri için veri madenciliği yapan bir tehdit.

- Cihazlara e-mail ile gelen bir zararlı link ile ya da girilen bir web sayfasından JavaScript kodu ile bulaşabiliriler.

- 2018'in ilke çeyreğinde yüzde 4000 artış olan bu tehdit türü gün geçtike hayatımızda daha çok yer alacaktır (Malwarebytes).

Hafta-9

İstismar Kitleri (Exploit Kit - EK)

- Truva atı, casus yazılım, fidye yazılımı gibi zararlı yazılımların oluşturduğu veri yüklerini (payload) dağıtmak için oluşturulan ve başarılı bulaştırabilmeyi maksimize eden bunu yaparken de popüler yazılımlardaki açıkların istismarını otomatik hale getiren araç kitleridir.
- Genellikle yönetim konsolu gibi çalışan bir EK, Adobe Flash, Java, Microsoft Silverlight gibi bilindik yazılımlardki açıklıkları hedef almaktadır.
- İstismar, bir sistemin açığını sömürerek ele geçirip bilgi toplamak amacıyla genellikle C, Perl, Python ve Ruby gibi yazılım dilleri kullanılarak oluşturulurlar.
- Rig, Neutrino, Magnitude ve Fiesta bilinen örnekler.

Hafta-9

İstismar Kitleri (Exploit Kit - EK) – Nasıl Çalışır

- **İrtibat**: Kurban, zararlı reklam, ele geçirilmiş bir web sitesi veya spam e-mail hiperlinki vsaıtasıyla bir EK sunucusuna bağlanan linke erişir.
- **Yönlendirme**: EK operatrötü tarafından belirlenmiş IP adresi veya web tarayıcı tipi gibi kriterlere göre kurban filtrelenir ve Ek'nın yer aldığı sunucuya yönlendirilir. Kriterleri karşılayamayan kurbanlar filtreleme ile elenir. Örneğin bir EK operatörü bir IP grubunu belirleyerek sadece belirli bir ülkenden gelecek kurbanları seçebilir. Ardından hangi açıkların istismar edileceğinin belirleneceği sayfaya yönlendirir.
- **İstismar**: Açıklar tespit edildikten sonra EK sunucusu açıpı olan uygulamları hedef almak için istismar dosyalarını indirir.
- **Bulaştırma**: Açıklar istimar edildikten sonra saldırgan Truva atı veya fidye yazılımı gibi zararlı yazılımları kurbanın makinesine indirir ve çalıştırır.

Hafta-9

İstismar Kitleri (Exploit Kit - EK)

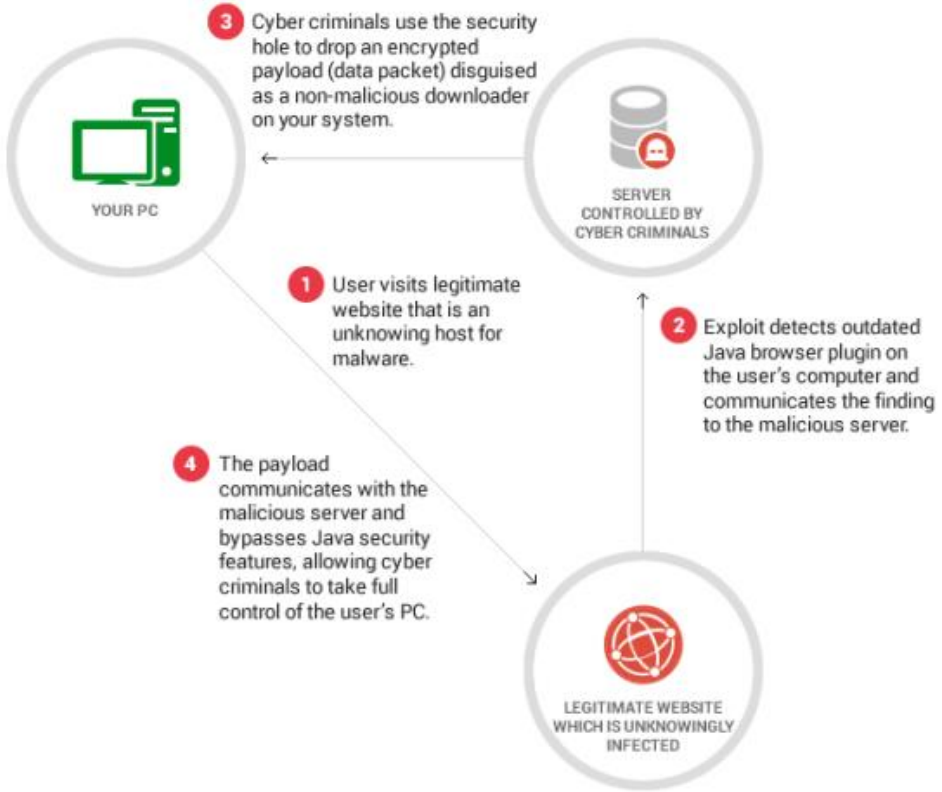
- CVE (Commoon Vulnerability Exposure) alenen bilinen problemler için ortak bir isimlendirme amacındaki bilgi güvenliği açığı ve hataları listesidir.
- Vulnerability; bir ağa veya sisteme erişim kazanmak için saldırgan tarafında kullanılabilecek yazılım hatasıdır.
- Exposure; bir ağa veya sisteme doğru atlama taşı olarak saldırgan tarafından kullanılabilecek bilgiye ve sistem kaynaklarına erişimi müsade eden yazılım hatasıdır.
- CVE ID formatında ilk dört rakam açığın tespit edildiği yılı , ikinci dört rakam ise o yıl tespit edilen kaçıncı açık olduğunu göstermektedir.
- Örneğin, CVE-2018-4878 : etkilenen yazılım 28.0.0.161 sürümüne kadar tüm Adobe Flash player, Ocak ve Şubat 2018 de ortaya çıkmıştır. MS Excel dökumanı içerisinde gömülü bir Flash nesne ile açık istimar edilmiştir. ROKRAT isimli RAT sonrsında sistem indirilip çalıştırılır.
- Örneğin; CVE-2013-2551: Microsoft Internet Explorer (6-10) ile ilgili bir açığı raporlamaktadır.

İnceleme Önerisi: https://www.cvedetails.com/vulnerability-list/

Hafta-9

Java Tabanlı İstismarlar

- Genellikle web tabanlı yazılım salrırılarının en yaygın şekli
- Enfekte edilmiş web sayfalarına girldiğinde burada bulunan ve yüklenmiş olan istismar kitleri devreye girecektir
- Güncellenmeyen Javanın güvenlik protokolerinin baypas edilmesi ile bilgsayarınızdaki açıkları tarayıp bilgileri çalma veya kontrolü ele geçirme



https://heimdalsecurity.com/blog/java-biggest-security-hole-your-computer/

Hafta-9

iFrame İstismarı

- iFrame HTML'in bir parçasıdır. HTML sayfasına vide, resim, dökuman ve reklam gibi ilaveler koyulmasında bir araç olarak kullanılır.
- iFrame istismarı HTML açıklarını kullanarak bir sayfanın içerisinde farklı bir internet sayfasını çağırıp, görüntülemenize yardımcı olan bir HTML etiketi olarak görülebilir.
- iFrame virüsleri sitenizin dosyalarına HTML kodu olarak yerleşir. Bu dosyalar: index.html, index.php, index.asp, default.asp, default.aspx, login.php, account.php
- Örneğin, mobil uygulamaların içerisine gömülerek farklı sunuculara siz farkında olmadan yönlendirilme işlemine maruz kalabilirsiniz.

Hafta-9

Water Holing

- İnsanların sıklıkla ziyaret ettiği sitelere olan güvenlerini istismar etmeye dayanan bir sosyal mühendilik saldırısıdır.
- Saldırgan tarafından popüler web sitesi ele geçirilir ve flash veya java client gibi açıkları istismar ederek ziyaretçilerin tarayıcılarına ya da işletim sistemlerine sızılır.
- İşletme veya kurumlar açısından su kaynağı saldırısı; hedef kurum kullanıcılarının en çok kullandığı dış siteler veya kurum sistemlerinin kullandığı dış kaynaklar tespit edildikten sonra bunlara zararlı yazılım bulaştırılması ve ardından asıl hedef olan kurum sitelerinin hedef alınması.

Hafta-9

Zero-Day

- İnsanların sıklıkla ziyaret ettiği sitelere olan güvenlerini istismar etmeye dayanan bir sosyal mühendilik saldırısıdır.
- Saldırgan tarafından popüler web sitesi ele geçirilir ve flash veya java client gibi açıkları istismar ederek ziyaretçilerin tarayıcılarına ya da işletim sistemlerine sızılır.
- İşletme veya kurumlar açısından su kaynağı saldırısı; hedef kurum kullanıcılarının en çok kullandığı dış siteler veya kurum sistemlerinin kullandığı dış kaynaklar tespit edildikten sonra bunlara zararlı yazılım bulaştırılması ve ardından asıl hedef olan kurum sitelerinin hedef alınması.

Hafta-9

- Ağlara Yönelik Tehditler
  - Hizmet dışı bırakma (DOS) Saldırısı
  - Botnetler ve DDOS
  - Port Yönlendirme ve Pivoting
  - Cybersquatting ve Bitsquatting
  - Paket Manipulasyonu
  - Spoofing
  - Oturum Çalma
  - Sahte Saldırılar
  - Parola Saldırıları
    - John the Ripper
    - THC Hydra

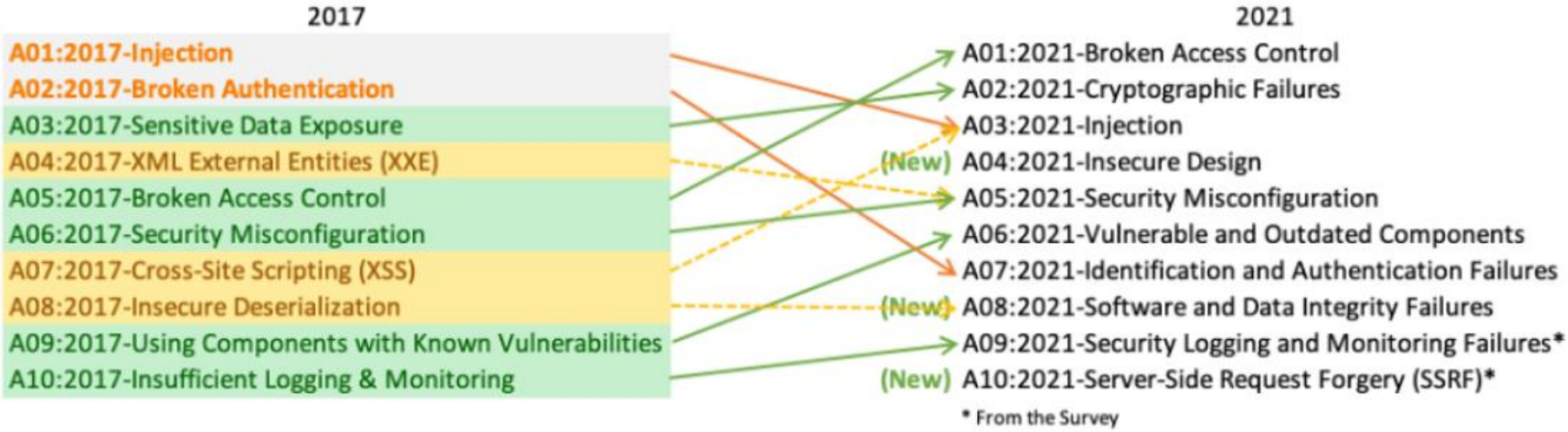
Hafta-9

Ağlara Yönelik Tehditler

- Açık Web uygulamaları güvenlik projesi (Open Web Application Security Project - OWSAP)

Top 10 Web Application Security Risks

There are three new categories, four categories with naming and scoping changes, and some consolidation in the Top 10 for 2021.



İnceleme Önerisi:
https://owasp.org/

Hafta-9

Hizmet dışı bırakma (DOS) Saldırısı

- Denial of Service-DoS: Hedef olarak belirlenen sistemin kaynaklarını tüketerek temel görevini yerine getirememesini sağlamak için yapılan ve bilgi güvenliğinde erişilebilirliliği hedef alan saldırı türüdür.
- DoS → tek bir kaynaktan hedefe yapılan saldırıdır
- DDoS (Distributed Denial of Service Attack) : Birden fazla kaynakla tek hedefe yapılan saldırı
- Saldırıda amaç sistemin kaldırabileceği yükün üzerinde anlık istek, anlık bağlantı ile sistemin cevap veremez hale getirilmesi veya hat kapasitesinin doldurulması suretiyle sistemin erişilebilirliliğinin ortadan kaldırılması
- Ayrıca hedef sistemlerde bulunan zafiyetler istismar edilerek, sistemin işleyemeyeceği şekilde bir istek gönderilir ve sistem erişilemez hale getirilir.
- Tipik DoS saldırılarında öne çıkan yöntemler şu şekildedir:
  - MAC Seli (Flooding)
  - ICMP Seli
  - ICMP Smurf
  - TCP SYN Seli
  - TCP Bağlantı Seli
  - UDP Seli
  - DHCP Açlık (Starvation) Saldırısı
  - Sahte/Yetkisiz DHCP Sunularıyla DoS
  - DNS Sorgusu Seli
  - HTTP GET Seli
  - SlowHTTP Saldırısı
  - Slowloris

İnceleme Önerisi: https://www.kaspersky.com.tr/resource-center/definitions/what-is-a-smurf-attack

Hafta-9

Botnetler ve DDoS Saldırısı

- Botnet: Robot ve network sözcüklerinin birleşiminden oluşur
- Saldırganlar Truva atları veya diğer zararlı yazılımları kurban adı verilen bilgisayarlara bulaştırarak uzaktan yönetebilecekleri bir bilgisayar ağı oluştururlar. Bu bilgisayarlar botnet üyesidir ve zombi yani köle bilgisayarlar olarak adlandırılırlar.

- Zombiler çevrimiçi oldukları müddetçe saldırganlar tarafınadan DDoS saldırısından kimlik hırsızlığına kadar birçok yasadışı aktivite için kullanılırlar.

- Botnetler dağıtık bir yapıdadır ve finansal dolandırıcılık, siber saldırılar, DDoS saldırıları, spam mail gönderme, yemleme-oltalama, phishing e-postaları, yazılımların yasal olmayan dağıtımları, bilgi ve kaynakların çalınması, kimlik hırsızlığı, online reklamlarda tıklama sahteciliği (click fraud) gibi birçok saldırı türlerini gerçekleştirebilirler.

İnceleme Önerisi:
STM Siber Tehdit Durum Raporu:
https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-ocak-mart-2021

İnceleme Önerisi:
N.E.Ş. Mehmet Kara, "Botnetlerle Mücadelede Dünyadaki ve Türkiyedeki durum", Malatya, 2011.

Hafta-9

Botnetler ve DDoS Saldırısı - Örnek

- Gamarue (Andromeda) isimli 2017 de durdurulan bir botnet (Microsoft)
- Durdurulana kadar 23 milyon farklı IP adresine bulaşmış
- 2011den bu yana 5 farklı versiyon: Petya ve Cerber fidye yazılımları, DDoS saldırılarında kullanılan Kasidet, Lethic spam botu, bilgi hırsızlığı yapan Ursnif, Caberp ve Fareit gibi birçok tehdidi dağıtmak için kullanıldığı tespit edilmiş
- Gamarue saldırı düzenlemek isteyenler için satılan bir kit olarak bilinir
- İlave plug-inler sayesinde fonksyionları da attırılabiilir örneğin:
  - Kullanıcı adı, parolalar veya finansal bilgileri çalmak için fare ve tuş takımlarındaki hareketleri kaydeden keylogger (150 dolar)
  - Gamarue'nin sürekliliği sağlamak için uygulamalara rootkit kodları enjekte eden bir Rootkit
  - Kurbanın bilgisayarını proxy sunucuya dönüştüren ve ağdaki diğer bilgisayarlara zararlı talimatlar gönderen Socks4/5
  - Web tarayıcılarına girilen bilgileri ele geçiren Formgrabber (250 dolar)
  - Kurbanın bilgisayarının uzaktan izlenmesi, dosya gönderilebilimesi için Teamviewer (250 dolar)
  - Taşınılabilir hard diskler ve flash diskler gibi taşınılabilir sürücülerle Gamarueyi yaymak için kullanılan Spreader

İnceleme Önerisi:
https://www.microsoft.com/tr-tr/security/business/security-intelligence-report

Hafta-9

Port Yönlendirme ve Pivoting

- Pivoting ele geçirilmiş sistem üzerinden farklı sistemlere saldırmaktır. Önce örneğin bir kurum ağına giriş izni olan bir makine ele geçirilir daha sonra diğerlerine ulaşım sağlanır.
- Pivoting işlemi port yönlendirme maksadıyla kullanılır. Port yönlendirmede, testi yapanlar ele geçirdiği bir hostu pivot olarak kullanmak suretiyle onun açık olan bir TCP/IP portuna erişir. Ardından pivoting metodunu kullanarak eriştiği bu porttan trafiği başka bir alt ağdaki (subnet) bir hostun portuna yönlendirir.
- Örnek olarak; bir kurumun dahili ağının dışından internet üzerinden saldırı yapıldığını düşünelim. Kurumun iç ağında arındırılmış bölgede (DMZ – Delimetered zone) bir sunucu olsun. DMZ güvenlik duvarı dışarıdan gelen harici trafiği filtreleyerek iç ağa girmesini engellerken, bu web sunucusunun tüm iç ağa erişimine izin verir. Dışarıdan özellikle açık olan 53 numaralı DNS portunu kullanarak bu web sunucusunu ele geçirebilirsiniz. Ardından bu porta gelen tüm trafiği özel ağdaki veri bankası sunucusuna port 22 (SSH) üzerinden yönlendirebilirsiniz. Bu özellikle DMZ de yer alan ve port engellemesi yapan güvenlik duvarlarını bypass etmenizi ve web sunucusunu kullanarak veri bankası sunucusuna erişmenizi sağlar.

İnceleme Önerisi:
https://resources.infosecinstitute.com/topic/pivoting-exploit-system-another-network/

Hafta-9

Cybersquatting ve Bitsquatting

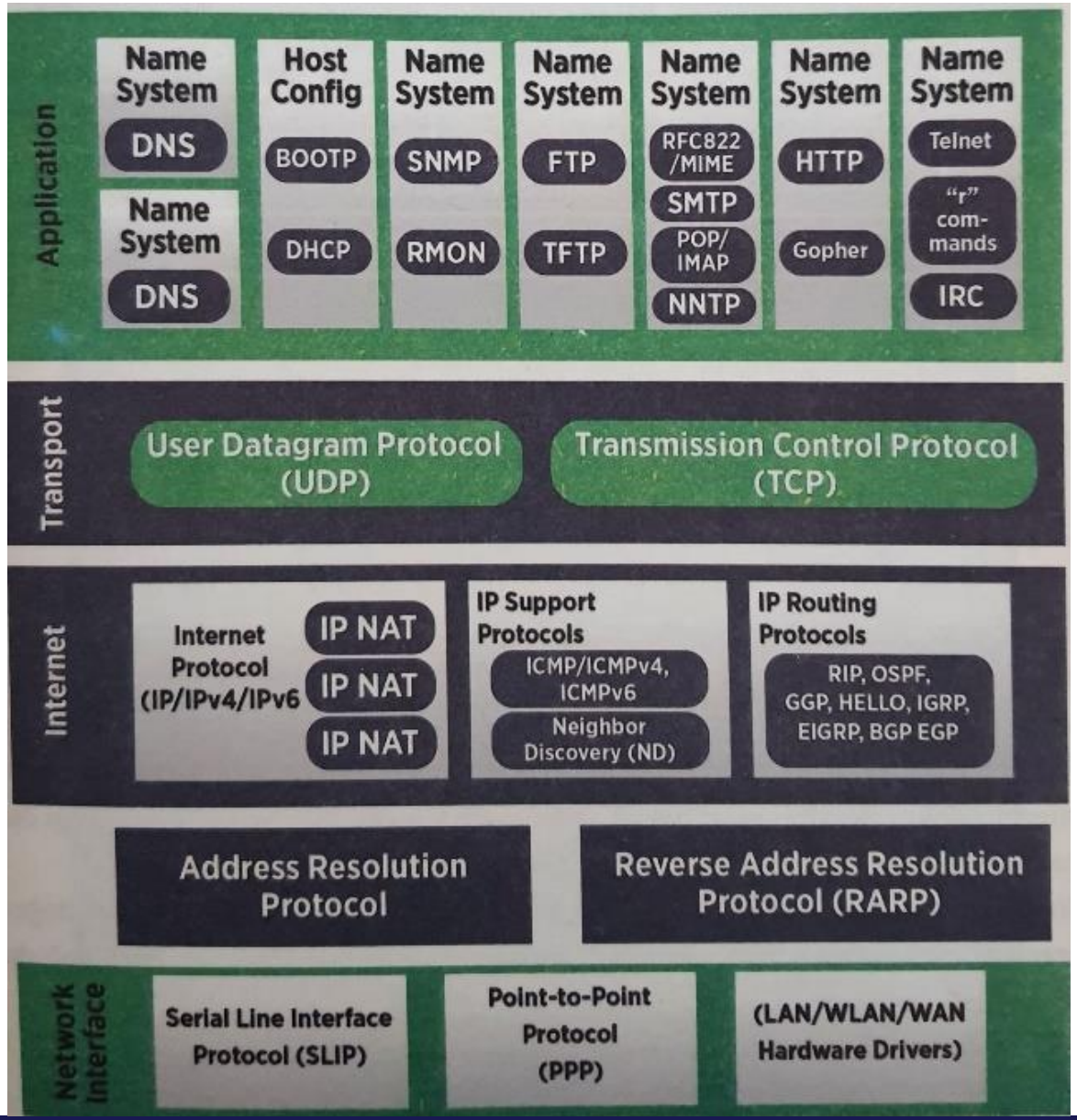
- Cybersquatting normalde var olan ve güncel olarak varlığını devam ettiren şirketlerin web alan adlarının farklı uzantılarını satın alarak, Bitsquatting ise web alan adlarından sadece bir bit farklı alanı satın alarak ziyaretçilerin kandırılması üzerine kurulu saldırı çeşididir.

Hafta-9

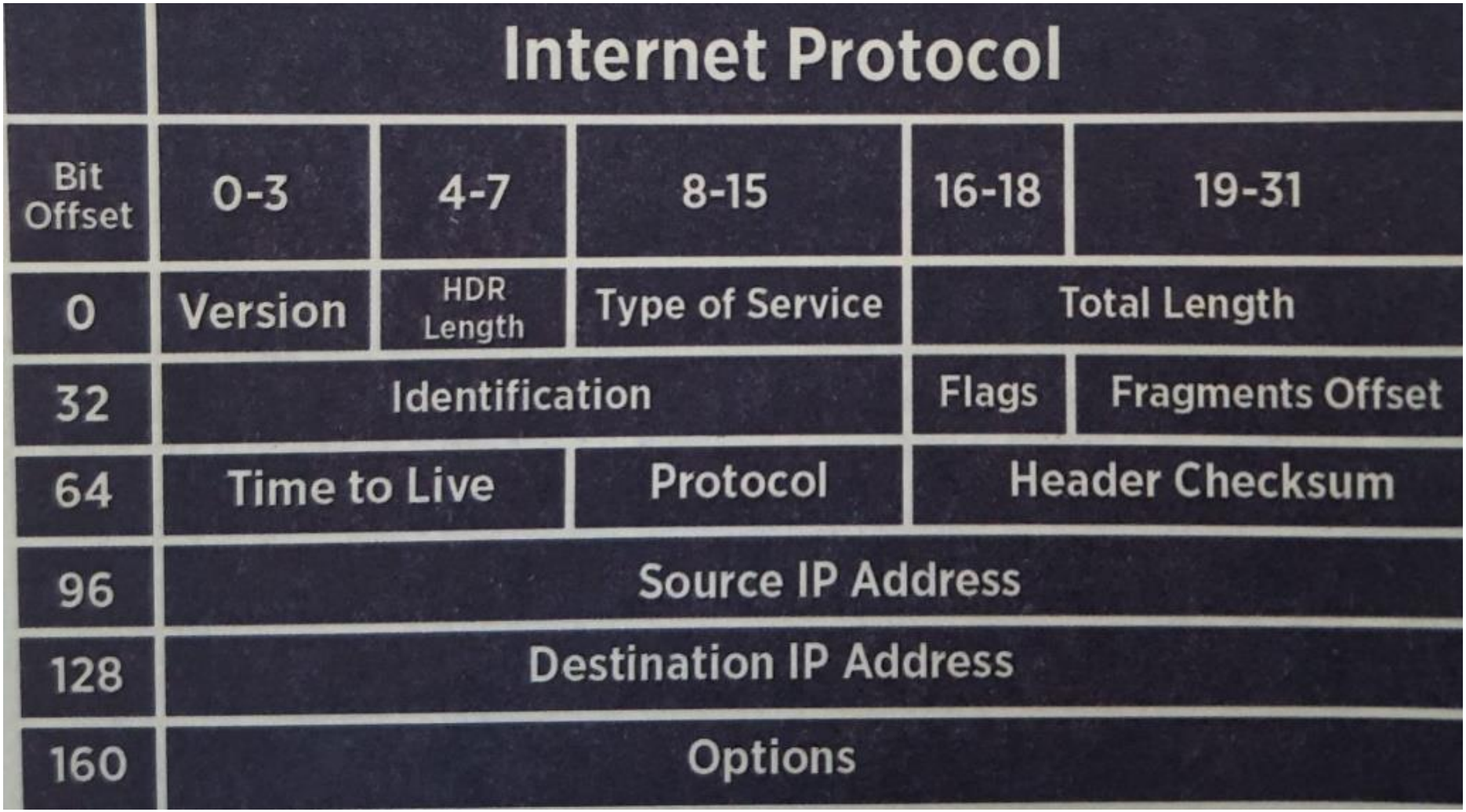
Paket Manipulasyonu

- Saldırgan ağa, bir iş istasyonuna veya sisteme giriş yaptıktan sonra, saldırı hedeflerinin sonraki katmanını belirlemek için bir listeleme (enumeration) saldırısı düzenler. Enumeration ilgili ağda bulunan diğer kaynakların listelenmesidir. Çalışan uygulama ve servisler, ağ cihazları, klasör ve dosyalar, ortak depolama alanları ve kullanıcı hesapları muhtemel saldırı listesinde yer alan kaynaklardandır.
- Enumeration bir talebe verilen cevap şeklindedir. Bu nedenle bu talepler paket manipülasyonu üzerinden gerçekleştirilir.
- Paket manipülasyonu yazılımı örneğin scapy: paket gönderme ve gönderilen paketin cevabını alma ve bu ikililleri listeleme (TCP/IP katmanında yer alan her protokol ve standart için paket tanımı yapabilir.)

TCP/IP Katmanları



IP Başlığı Alanları



	Internet Protocol				
Bit Offset	0-3	4-7	8-15	16-18	19-31
0	Version	HDR Length	Type of Service	Total Length	
32	Identification			Flags	Fragments Offset
64	Time to Live		Protocol	Header Checksum	
96	Source IP Address				
128	Destination IP Address				
160	Options				

Hafta-9

Spoofing

- Genel olarak saldırganın kendisine ait olmayan bir adresi ve kimlik bilgilerini kullnarak yaptığı saldırılardır.
- E-mail spoofing
- IP spoofing
- ARP spoofing
- MAC spoofing
- DNS spoofing

Hafta-9

Spoofing

- Genel olarak saldırganın kendisine ait olmayan bir adresi ve kimlik bilgilerini kullnarak yaptığı saldırılardır.
- E-mail spoofing
- IP spoofing
- ARP spoofing
- MAC spoofing
- DNS spoofing

E-mail spoofing. E-mail başlıklarının değiştirilmesi suretiyle iletinin orijinal göndericisi yerine başka bir yerden ya da kurumdan geliyormuş gibi gösterildiği bir tür sahteciliktir. SMTP protokolünün eksikliklerinden dolayı, gönderici adresini herhangi bir kişi, kurum veya organizasyon olarak ayarlayıp e-mail göndermek mümkündür.

Hafta-9

IP spoofing

IP spoofing. Saldırgana ait olmayan belirlenecek herhangi bir IP adresinden TCP/IP paketleri *(tcp, udp, ip, icmp, http, smtp, dns vb.)* gönderebilme işlemine IP sahteciliği *(IP spoofing)* denir. IP protokolünde herhangi bir doğrulama mekanizması olmadığından sahte IP paketini alan taraf paketin gerçekten gönderilen IP adresinden gelip gelmediğini bilemez. Teorik olarak IP sahteciliği tüm protokollerde mümkün gözükse de pratikte sadece UDP kullanan uygulamalarda gerçekleştirilebilir. Başlık bilgisinde yer alan sıra numaraları tahmin edilemez şekilde üretildiğinden TCP tabanlı uygulamalarda gerçekleştirilemez. TCP, bağlantı öncesi her iki uç arasında üçlü el sıkışma gerektirdiğinden bu aşamaları geçmeden iki uç arasında veri transferi normal yollardan gerçekleştirilemez.[43]

Hafta-9

ARP spoofing

- ARP spoofing. ARP yerel ağdaki IP adreslerini MAC adresleriyle eşleştiren bir protokoldür. Ağdaki bir bilgisayar, paket göndereceği başka bir bilgisayarın MAC adresini öğrenmek için anahtara *(switch)* ARP isteği gönderir ve anahtar bu paketi tüm portlarından *(broadcast)* ağa gönderir. Bu ARP isteğine sadece paketin gönderileceği hedef bilgisayar cevap verir. Ardından paketi gönderen bilgisayar bu IP-MAC eşleşmesini kendi ARP tablosunda tutar.

Hatırlanacağı üzere ARP isteğine sadece paketin gönderileceği bilgisayarın cevap vermesi gerekiyordu. ARP sahtekârlığında *(ARP spoofing, ARP flooding, ARP poisoning)* saldırgan, paketin gönderileceği bilgisayarın yerine ARP isteğine cevap verir. Neticesinde, paketi gönderen bilgisayarın ARP tablosunda *(IP-MAC eşleşmesi tablo-*

Hafta-9

ARP spoofing

su) saldırganın bilgisayarının IP ve MAC adresleri bulunur ve paketler hedef bilgisayar yerine saldırganın bilgisayarına gönderilir. Saldırganın varsayılan ağ geçidinin *(default gateway)* yerine ARP isteklerine cevap vermesi durumunda ise ağdan çıkacak olan tüm paketler, varsayılan ağ geçidi yerine saldırganın bilgisayarı üzerinden dışarı çıkacaktır. Böylece saldırgan ağdan çıkan tüm paketleri bir paket analizörü ile takip edebilir.[44]

Hafta-9

MAC ve DNS spoofing

MAC spoofing saldırısında saldırgan, anahtara *(switch)* gönderdiği çerçevelerin *(frame)* içerisindeki "kaynak MAC adres" kısmına, dinlemek istediği bilgisayarın MAC adresini yazar. Anahtar MAC adres tablosunu bu duruma göre günceller. Böylece anahtarın MAC adres tablosunda, saldırganın bağlanmış olduğu anahtarın portu için iki adet MAC adresi yer almış olur *(Saldırganın MAC adresi ve hedef bilgisayarın MAC adresi)*. Hedef bilgisayara gönderilen çerçeveler de *(frame)* böylece saldırganın bilgisayarına gönderilmiş olur.

DNS spoofing, bir alan adı sistemi *(Domain Name System-DNS)* sunucusunun ön bellek veri tabanına veri eklenerek ya da oradaki veriler değiştirilerek DNS sunucunun yanlış IP adresleri dönmesine ve trafiğin başka bir bilgisayara *(sıklıkla da saldırganın bilgisayarına)* yönlendirilmesine neden olan bir saldırıdır.[45]