OSI Katmanları

Layer 1,2,3,4,7
(5 6, 7 ye dahil denebilir)

Application, uygulama. (FTP, SSH, telnet, SMTP, HTTP, DNS)
Presentation, fotoğrafları network paketlerinin taşıyabileceği şekile çeviriyor.
Session, tcp tünelleri, sertifikasyon vs.
Transport, karşıya nasıl gönderilecek (TCP, UDP)
Network, nereye gideceğim? Gönderici ve alıcı, kimlik, lokasyon. Ip adresi layer3 de kararlaştırılıyor.
Data Link, (NAT kontrolü) kimlik MAC bilgileri, hangi cihaz üzerinden gideceği, nereye uğrayacağı vs mac kimlik bilgileri.
Physical, wifi, kablo, bluetooth, kızılötesi somut aracın kendisi.

Tcpdump

- Farklı ara yüzlerden, portlardan ve protokollerden trafik toplar.
- UDP paketlerini de işleyebilir.
- Çıktısı stdout türevidir, piping operasyonları ile parse edilebilir.
- Wireshark için pcap dosyası yazabilir.

UDP'de payload'ı da görebiliyorsunuz, TCP'de görünmüyor.

Netsniff-ng (engine)

- Interface'ler üzerinden trafik toplamak üzere geliştirilmiş bir uygulamadır.
- Kernel-copy mantığı ile çalıştığından dolayı, ciddi derece de hızlıdır.
- Bir çok NIDS yazılımı, modül olarak bu uygulamayı kullanır.
- C dili ve open-source, bu yüzden geliştirilmeye müsaittir.

Wireshark

Farklı arayüzleri dinleyebilir.
Paket içeriklerini gözlemleyebilir.

*Timestamp
*Kaynak
*Hedef
*Protokol

Ve taşınan veriler hakkında bilgi sunabilir.

NETWORK PAKET İZLEME

Network Paket Yapısı

Frame, Layer 1 tarafında kablo üzerinden geçmekte olan en basit paket wrap katmanıdır.

Ethernet II adı ile anılmakta olan katman, Layer 2 tarafının temsilcisi olarak düşünebilir. Hedef ve kaynak MAC adreslerinin tanımlandığı kısım burasıdır.

Internet Protocol (IP) anlatımlarının bulunduğu kısım, Layer 3 tarafını kastetmektedir. Paketin IP Adresi bilgileri, bu süreç dahilinde verilir.

ANALİZ

DHCP Exhausting and Starvation

DHCP, ağa bağlanan cihazlara, IP adresi, ağ maskesi, DNS sunucusu, varsayılan ağ geçidi gibi gerekli bilgi ve kimlikleri otomatik olarak veren bir sistemdir. Bir cihaz ağa bağlandığında DHCP sunucusuna haber verir, ve ihtiyacı olan bu bilgiler ona verilir.

DHCP Starvation

DHCP Starvation saldırısı ise, bir ağın DHCP sunucusunu IP adresi dağıtamaz hale getirerek, ağa bağlanan yeni cihazların kimliksiz kalması için yapılmaktadır. Eğer ağa fazlasıyla DHCP Request paketi gönderildiyse, bir zaman sonra DHCP Sunucusu sahip olduğu tüm ip adreslerini saldırgana vermiş olacak, ve elinde IP Adresi kalmayacaktır. Bu yüzden DHCP Starvation, bir hizmet engelleme saldırısı olarak kullanılabilir.

DHCP, mac adresini veriyorsun, IP adresi veriliyor.
C sınıfı EV 254 ip adresi
B sınıfı büyük 254x254 = 64.516 ip adresi

Hizmet reddi (DoS) saldırısı.

Analiz kısmında Timestamplere dikkat edeceğiz. DHCP tüketme saldırısı, script tarafından hızlı şekilde yapılır.
İstatistikler -> DHCP -> DHCP Discover (1) , Offer (Ip'nin verilmesi),
dhcp contains request

Network'de az kişi var çok fazla discover var.
Timestampler çok sık. Discover var.

SQLi Saldırısı

SQL Query dilleri, veri tabanı sistemleri üzerinde bazı işlemler yapmak maksadı ile kullanılan kodlardan ve komutlardan oluşur.

SQL dillerinde tek veya çift tırnak (',") olarak adlandırılan karakterler; girdilerin, objelerin, verilerin veya querylerin etrafını sararak, onların tanımlanmasını sağlamaktadırlar.

URL encode hali %27 olan tek tırnak(') karakteri olacaktır. Wireshark üzerinde girdi olarak verilebilen doğru bir filtreleme, içerisinde bu karakterin geçtiği HTTP paketlerini izleyebilir ve saldırının yürütülmesinde rol oynayan Request'leri tespit edebilir.

!ocsp && http && (http contains "GET" || http contains "POST") && http contains "%27"

Time Based sql'de parantez ve sleep'leri bulmak gerekir.
Sleep 20, 22 sn. sonra döndüyse timebased vardır.

Nmap

Nmap uygulamasının ana misyonlarından biri, hedeflenen sistem üzerinde çalışmakta olan portların aktifliği tespit etmektir. Bu portlar hem TCP, hem de UDP yapılarına sahip olabilirler. TCP uyg. çok daha büyük oranda kullanımda olması göz önüne alındığında, bir saldırganın öncelikle TCP bazlı bir tarama yapacağı rahatlıkla tahmin edilebilir.

TCP protokolü, yapısı gereği Three Way Handshake algoritması kullanır. SYN ve ACK paketleri burada ön plandadır.

SYN, SYN-ACK, ACK, ESTABLISHED

!icmp && tcp && tcp.flags.syn==1 && tcp.flags.ack==0 && tcp.dstport > 65500

SSH Brute Forcing

SSH Servisi, ilgili makine üzerinde güvenli bir biçimde kod çalıştırılmasına yarar.

Servisin üzerinde doğru bir güvenlik yapılandırması kurgulanmadıysa, saldırganlar sistem üzerinde bulunan hesapları ele geçirebilmek adına rahatlıkla kaba kuvvet saldırıları gerçekleştirebilirler.

Bir ağ trafiği incelendiğinde, eğer belli ve kısa bir zaman içerisinde çok fazla anahtar takas paketi görülmekte ise, burada bir kaba kuvvet saldırısı olduğundan bahsedilebilir.

ssh && tcp.dstport == 22 && frame.len == 1346

Wifi Deauthentication

Deauthentication, yani yetkisizleştirme saldırıları, AP olarak adlandırılan kablosuz erişim noktalarına yapılmaktadır. Bu saldırıda amaç, hedef AP cihazına yetkisizleştirme iletileri göndererek, bu cihaza bağlı olan kullanıcıların bağlantılarını koparmak ve bu şekilde kablosuz haberleşmeyi engellemektir. Aynı zamanda bu saldırı sonrasında, ilgili kullanıcı cihazlarının tekrar bağlanmaya çalışması ile birlikte belirli veriler yakalanarak, şifrelenmiş veri üzerinde parola deneme işlemleri yapılabilmektedir.

aireplay-ng -0 5 -a 1C:67:58:9C:6F:12 -c 1C… wlanm0n

wlan.ssid
(wlan.fc.type == 0) && (wlan.fc.type_subtype == 0x0c) // deauthları bulmak için bir query
eapol // eapol protokolünü filtrele, 4 aşamalı

Deauth istekleri çok sık olmaz. Timestamp'den saptanabilir.
Bu istekleri gönderen kişi ne access point ne de ip'si ağda yoksa saldırgandır.

VOIP Sniffing

Voice Ip Yapıları, kendi aralarında iletişim gerçekleştirebilmek adına TCP/IP yöntemlerini kullanırlar.

Sniffing mekanizmalarını doğru filtrelemeler ile yapılandırılabilmiş bir saldırgan, haberleşmekte olan VOIP cihazları arasındaki trafikleri koklayarak geçen RTP paketlerini elde edebilir ve paketlerin birleşimleri ile bir yayın oluşturarak konuşmaları dinleyebilir.

Aynı zamanda RTSP paketlerini yenileyebilen bir saldırgan, ilgili yayımlar üzerinde kontrol sahibi olabilir. Bu gibi durumlardan korunmanın en kolay ve mantıklı yolu, şifrelenmiş iletişimler kullanmaktır.

(UDP, ses ve video, konf. Hızlı old. İçin)
MITM, sniff veya sadece sniff. Çağrıları başlatan durduran paketlerdeki RTSP bayraklarıdır.
RTP paketleri de ses dosyalarını taşır.
Eğer RTP paketlerini wireshark da doğru sırada RTP Player'a atılırsa konuşma dinlenebilir.

İki tarafın RTP paketleri aynı şekilde sıralanabilir, konuşma olduğu gibi dinlenebilir.

PacketTotal
PacketTotal, ağ paketi topluluklarını çevrimiçi olarak inceleyebilen bir servistir.
Virüs totalin network analiz versiyonu, pcap dosyası atılabilir.

Paket topluluklarını DHCP, DNS, SSL ve benzeri paket türlerine göre filtreleyebilir, zaman, kaynak, hedef, metot gibi alt başlıkları gösterebilir.

Paketler içerisindeki IP Adreslerinin private veya public olduğunu tespit edebilir, uygun olanların whois veya geolocation bilgilerini sorgulayabilir.