Ağ Haritaları (Network Maps)

Hub

Verinin tek cihaza gönderilmesi gerekirken bütün cihazlara göndererek cihazları meşgul eder. OSI Layer1'de çalışır. Basit elektronik devre kartından oluşur.

Switch

Anahtarlamalı veri akışı sunar. Veri sadece iki cihaz arasında akar, diğer cihazlara gönderilmez. ARP tablosu kullanır. Normalde Layer2, eğer routing'de yaparsa Layer3'te çalışır.

Snooping ve Sniffing (Gözetlemek ve Koklamak)

Ağ trafikleri arasında beliren bir haberleşmeyi dinlemek.

Spoofing

Spoofing, herhangi bir IP adresi üzerinden TCP/IP paketleri gönderebilme işlemine verilen isimdir. Genel olarak kendisini daha yetkili şekilde tanımlamak için kullanılır.

Poisoning Nedir?

MITM (Man-in-the-Middle) (Ortadaki Adam) gerçekleştiği birçok durum, zehirlemeler sonucu arz olmaktadır.
(e.g P2P mimarisi için, whatsapp uçtan uca şifreleme, iki ucun arasına girebilirsek MITM)

Misconfigs

Hatalı yapılandırmalar sonucunda, P2P -> broadcast'e dönüşür. İstenmeyen kişiler tarafından incelenebilir.

Wi-Fi Sniffing

Adaptör modunda bir NIC kullanan saldırgan, havadaki sinyal trafiği dahilindeki bazı değerleri izleyebilir ve bunları saldırı vektörleri hazırlama fazlarında kullanabilir.

ARP Protokolü (Address Resolution Protocol)

Cihazların birbirini tanıması için, IP ve MAC adresleri bir tabloda tutulur.

ARP Cache Poisoning / Spoofing

Haberleşen cihazlara sahte kimlik bilgileri göndererek, kendini ağdaki başka bir cihaz gibi tanıtabilir ve bu sayede haberleşmenin kendi üzerinden gerçekleşmesini

sağlayabilir. Bu saldırı, özellikle şifresiz trafiklerin açığa çıkması durumunda çok etkilidir. Bu vektör ile kişi, şifreler, e-postalar gibi kritik verileri okuyabilir. Kurban, saldırganı switch zanneder. (MITM)

DNS Poisoning / Spoofing

DNS, kendisine verilen bilgisayar veya web sitesi ismini ulaşılmak istenen bu ismin ikamet ettiği IP adresine çeviren sistemdir. Yani, ismi verilen cihazın adresini bulmak için kullanılır.

DNS Spoofing, yani DNS Önbellek Zehirlemesi ise, ağ içerisinde yapılan bir DNS isteğinin manipüle edilmesidir.

Network Mapping

Sniffing, ağ haritalarının hızlı bir şekilde çıkarılabilmesi için iyi bir yöntemdir.

LB (Load Balancer) / Appsrv (Application Server) Traffic

Bazı durumlarda ağ yapıları içerisindeki trafik mecburen şifrelenmemiş olmak zorundadır. Load Balancer, Front-end Server veya web proxy mekanizmalarının kullanıldığı yapılar, bu duruma örnek olarak gösterilebilir. Bir LB sunucusunun kullanıldığı fazda, HTTPS paketlerinin bir şekilde açılması ve okunması, log mekanizmalarının doğru çalışması için gereklidir. Aynı şekilde IDS ve WAF yapıları da; trafiğin HTTPS olması durumunda paketlerin içeriklerini okuyamazlar ve olası saldırılar fark edilemez.

HTTP Header Hijack

Eğer yapı dahilindeki HTTP paketlerinin yük kısımları özel bir şifreleme yapısına tabii tutulurken, Request ve Response paketlerinin Header bilgileri, bazı durumlar dolayısı ile bu şifrelemeye tabii tutulmaz ise başarı ile gerçekleştirilmiş sniffing vektörleri, ilgili paketler üzerinde geçen kritik anahtarları yakalayabilirler. Authentication, X-Forwarded-For, CustomAccessKey, Location gibi başlıklar, bunlara örnek olarak verilebilir.

TCP Session Hijacking

Cleartext üzerinden işlem yapmakta olan protokoller, güvenlik yapısı olarak zayıflardır. Bu gibi iletişimlerin güvenli hale getirilebilmesi için, genellikle ağ dahilindeki yetkilendirilmeler düzenlenir ve one-time-password yapıları kullanılır. Örneğin, eğer SKEY ile one-time-password özellikleri kullanılmakta ise, saldırgan ilgili iletişim

dahilinde sniff ettiği parolayı; zaten daha önce kullanıldığı için bir kez daha kullanamaz.

TCP Session Hij. zafiyetleri, bu gibi durumlar dahilinde devreye girer. Sniffing saldırısını başarı ile gerçekleştiren saldırgan, tespit ettiği SEQ numarasını kullanarak ilgili TCP sezonunun kontrolünü ele geçirebilir.

Log Suppressing

Saldırganlar başarılı sniffing ve poisoning vektörlerini kullanarak, başta NIDS ve Log Management gibi yapıları kandırmak için aksiyonlar alabilirler. Bu gibi yapılar, kendilerine gelen paketleri işler ve bunun sonucunda bir elde ettikleri kayıtları gözden geçirerek benzer alarm bildirimleri üretir. Bu paketlerin iletim kontrollerine müdahale edebilen saldırgan, paketlerin iletimini engelleyebilir ve alarm üretiminin önüne geçebilir - dolayısı ile farkındalığın kırılmasına sebebiyet verebilir.

VoIP

VoIP, IP üzerinden ses, video veya mesaj gönderilmesidir. İnternet veya bilgisayar ağları üzerinden çalıştığı için genellikle daha ucuz, bazen bedavadır. Bu nedenle günümüzden en çok tercih edilen telekomünikasyon iletişim yönetimidir. VoIP, sesinizi internet üzerinde yolculuk yapan dijital sinyallere çevirir.

- Bknz: VoIP Sniffing

Turtles

- LAN Turtle - Hak5

LAN Turtle, basit bir grafik kabuk aracılığıyla gizli uzaktan erişim, ağ istihbaratı toplama ve ortadaki adam gözetim yetenekleri sağlayan gizli bir Sistem Yönetimi ve Sızma Testi aracıdır. Genel bir "USB Ethernet Adaptörü" kasası içinde yer alan LAN Turtle'ın gizli görünümü, birçok BT ortamına uyum sağlamasına olanak tanır.