SSH & SCP

SSH Tunelling

Yapısı gereği şifrelenmiş bir trafik iletimi sunar.
Sniff saldırı vektörlerine karşı ciddi manada koruma sağlar.

Bağlanılmak istenen sunucuya başka bir sunucu üzerinden şifrelenmiş bir trafikle bağlanma şeklidir.

Yerel Port Yönlendirme
Uzaktaki makinenin bir servis portunu, SSH ile local makinede sunmaktır.
*İlgili servis, HTTP olabilir.
*CloudFlare gibi bir proxy kurulabilir.

Uzak Port Yönlendirme
Local makinede çalışan bir uygulamanın uzaktaki bir makine üzerinden yayılması durumu.

Dinamik Port Yönlendirme
Trafiğin öncelikle bir SSH sunucusuna iletilmesine, sonrasında ise oradan dağıtılmasına izin verir.

Public Key Pair

Bu yöntem ilgili veriyi şifrelemek ve şifreyi çözmek için iki farklı anahtar kullanır. (public, private key)

SSH Bağlantıları dahilinde parola kullanımı aktif olur ise, her ne kadar güvenilir bir parola oluşturduğumuzu düşünsek de, saldırganlar uzun mesailer harcayıp bu parolaları tahmin etmeyi başarabilirler.

Ancak SSH bağlantısı her kurulduğunda parola yerine sertifika yöntemi kullanılır ise, bu tahmin durumu pratik olarak neredeyse imkansız olacaktır.

SSH Sıkılaştırma

Bir güvenlik önlemi olarak, standart olan 22 port numarası değiştirilmelidir.
<PermitRootLogin> parametresine <no> değeri atanmalı, root kullanıcısının SSH bağlantısı yapmasını engellenmelidir. Böylece başarılı bir kaba kuvvet saldırısı gerçekleştirebilen saldırganın en yetkili kullanıcı olarak sisteme bağlanması engellenebilir.

X11 Forwarding parametresine <no> değeri atanır ise, Port yönlendirme devre dışı bırakılabilir.

SCPOnly Shell

SCP aracı ise, aynı teknolojiyi kullanarak güvenli bir şekilde dosya transferi yapılmasını sağlayan SSH'ın yardımcısı bir araçtır. Burada doğabilecek problem ise, SCP aracını kullanırken girilen yetkilendirme parolasının, SSH aracını kullanır iken girilen parola ile aynı olmasıdır. Yani bir kullanıcıya SCP aracını kullanması için hesap bilgileri verildiğinde, o kullanıcı aynı şekilde SSH bağlantısı kurabilecek ve sistem üzerinde komut çalıştırabilecektir.

Bu durumun önüne geçmek ve kullanıcıya sadece SCP işlemleri gerçekleştirebilen bir terminal verebilmek; SCP-Only Shell terimi geliştirilmiştir.

SCP-Only Shell, güvenlik gereksinimleri doğrultusunda yetenekleri kısıtlanmış olan bir Shell türevidir. Amacı, kullanıcının komut çalıştırma yeteneğini kısıtlamak, kullanıcının sadece SCP ile alakalı; dolayısı ile sadece dosya transferi ve türevi işlemleri yapabilmesini sağlamaktır.

Firewalld & UFW

Rich Rules

Bazı durumlarda, firewalld konfigürasyonu daha güçlü bir hale getirmek veya duruma özel ihtiyaçları karşılamak için, sadece belli servis ve portlar üzerinde değil, IP Adresi bazlı yetkilendirmeler de yapılmalıdır. Rich rules, sistem üzerinde daha detaylı ve spesifik ayarlar yapabilmemiz için yardımcı olur.

Firewall-cmd --zone=public --add-rich-rule="rule family=ipv4 source address=192.168.1.56 service name=ssh reject"

Firewall-cmd --zone=public --add-rich-rule="rule family=ipv4 source address=192.168.1.56 port protocol=tcp port=4000 reject"

Firewall, ip spoofing'e zaafı vardır.

Reverse_packter filtering (rp_filter)
Gelen paketi trace edip gönderildiği iddia edilen yere sorar bunu gönderdin mi? Eğer spoof'sa göndermemiş olacağı için paket iptal edilecektir.

SSL & TLS
Self Signed
(HTTP & HTTPS)
CA Trusted, otoriteler tarafından tanınan sertifikalara verilen isimdir.
Self sign ise otoritelerin henüz tanımadığı ve sistem yöneticileri tarafından oluşturulmuş SSL veya TLS sertifikalarıdır.

Chippers

SSLv2, SSLv3 ve TLS 1.0 desteği devre dışı bırakılmalı ve sadece TLS 1.1 ve 1.2 desteklenmelidir.

Şifreleme ve doğrulama desteği vermeyen NULL aNULL eNULL cipher suiteleri devre dışı bırakılmalıdır.

Diffie-Hellman özell sahip cipher suiteler tercih edilmelidir. Perfect Forward Secrecy isminde önemli bir özellik sunar ve bu sayede SSL anahtarının güvenliği ihlal edilse bile, geçmişteki trafiğin çözülmesini engeller.

Downgrade Attacks

MITM saldırıları dahilinde, eğer saldırgan ilgili trafiği zehirleyebilirse, kendi üzerinden akmakta olan ve sniff ettiği tüm trafiği manipüle de edebilir. Downgrade saldırılarında, basit bir senaryo ele alınır ise;

Sunucu, hem HTTP hem de HTTPS olarak hizmet verebilmektedir. Google gibi web arama motorları tarafında ise tabii ki HTTPS index'ler kayıtlıdır. MITM saldırısı altında olan istemci, her zaman olduğu gibi https://test.com/ adresine giderken, saldırgan bu trafiği manipüle eder ve paketin hedef port numarasını HTTP portuna denk gelecek şekilde değiştirir.

Bu durumda, sezon yapısı artık HTTP üzerinden kurulacak ve günün sonunda saldırgan, ilgili tüm trafiği düz metin olarak izleyebilecektir.

Saldırının, HTTPS sertifikaların gücünü düşüren, sertifikaları değiştiren, proxy olarak traffic redirecting yapan türleri de vardır.

HSTS
HSTS -> HTTPS e zorlama, HTTP kabul etmeme.

HPKP
HTTP Public Key Pinning
Kullanıcının tanımlanmış başlık bilgisi (sertifika) dışında kabul etmez. (Burp, proxy red eder)

SSL Certificate Pinning
Mobil ve masaüstü uyg, yapıları gereği REST API sistemleri ile çalışırlar. Bu yazılımlar üzerinde Fuzzing işlemini başarıyla tamamlayan bir saldırgan, arkada çalışmakta olan API sistemini rahatlıkla keşfedebilir. Bu durumun önlenmesi için, aradaki trafiğin saldırgan tarafından anlaşılmaz hale getirilmesidir.

Cert Pinning'de, uygulama içerisine sertifikaya ait parmak izi gömülür.

802.1x
NAC, sunucular ile yapılır.
Port Security, switch veya firewall ile olur.
EAP.
(Bir kimlik denetleyici SW veya AP, bir de kimlik denetleme sunucusu RADIUS)

Port Security - MAC Filtering
Ofansif Açılar ve Korunma
Saldırganlar, bu kontrolleri atlatmak için MAC adreslerini maskelese bile, paketlerin gönderildiği IP adresi aynı kalacaktır.

Salgırgan, aynı zamanda taklit ettiği MAC adresine karşı gelen IP Adresini de spooflar ise, bu sefer de aynı IP adresi ağda 2 farklı makinede aynı anda bulunacaktır.

Eğer hem MAC hem de IP Adresini spoofladığı esnada orjinal makineye ağda bulunmuyor ise, bu sefer de DHCP kayıtlarına bakılması gerekmektedir. Eğer bu makineye DHCP yapılmadı veya çok uzun zaman önce yapıldı ise, paket yine engellenmelidir.

Rate Limiting, saniyede 600 istek geliyorsa, bağlantısını kes. (örn.)

SQL Sunucuları Privileges

İlgili makinelere olan erişim, sadece DMZ, bazı durumlarda ise sadece LAN üzerinden gerçekleştirilebilmelidir.

Servis kullanıcılarının yetki seviyeleri seviyeleri doğru ayarlanmalıdır, uygulama yüksek yetkilerle çalışmamalıdır.

Veri tabanı sistemleri; Select, insert, update, delete, exec, write vb. gibi, kayıtlar hakkında farklı işler yapabilecek fonksiyonlara sahiplerdir.

Injections

Prof. Bakış açısında geliştiricilerin, işi mekanizmaların çalışması için gereken programlamaları üretmek ve bunların sürekliliğini sağlamaktır.

Proxy, API Gateway, Frontend-Server vb yapıları kullanmak, yönetilebilirliği ve yük dağıtımını pozitif olarak etkileyecektir.

Bu gibi durumlarda, veri tabanı sistemleri ile iletişime geçmekte olan yapıların üzerinde güvenlik önlemleri alınması microservices felsefelerine ve mimarisine aykırı bir bakış açıcı olarak ve geliştiricilere efor sarf ettirecektir. Bu durumda yazılımlar, monolitik sınıfa geçerler.

Önlem, SQL eventleri geliştirilmeli ve inj önlemleri alınmalıdır.

Master & Slave

Master telefon, powerbank slave (backup)

Mod Security

Ücretsiz WAF, Apache, nginx ve IIS 'de kullanılabilir.

Mod_evasive

DoS veya Brute-Force
10sn 8den fazla request olursa ona 40 sn ban at.

Fail2Ban

SSH Brute forcing engeller.
Çok fazla faile BAN!

Disk Şifreleme

Bitlocker, veya encrypted LVM

Diski sök başka cihaza tak disk tanıyamayacak.

Backup Mimarisi

Yedekleme sunucuları merkezi sunucularına bağlanmamalıdır.
StandAlone çalışmalıdır.

Statik crontab yapıları devre dışı olmalı, rastgele zaman ayarları olmalıdır.

Alınan yedekler üçüncü parti ve lokasyonda barındırılmamalıdır.

Harici yedekler, disklere ve teyp bantlarına gömülmelidir.

IDS & Proxy

Log Management

Dosyaların hashleri sürekli calculate eder.
Örn. Etc.passwd