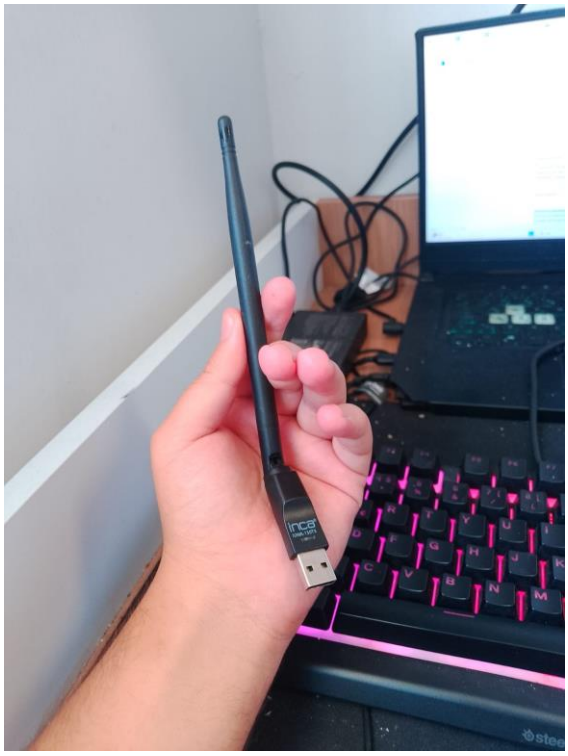
Wireless Attack saldırıları

Wireless attack saldırılarının birkaç şekli vardır. Ana amaç kullanıcının bilgilerini ele geçirmektir. Buradaki çöğu saldırıyı yapabilmek için elinizde olması gereken bir araç vardır. O da Usb Wifi karttır. Benim elimdeki kart bu şekilde eğitim amaçlı saldırıları gösterebilirdim lakin şimdilik sözlü anlatacağım.



Kullanılan Araçlar ve Toollar:

1. Wi-Fi Kartı (Wireless Network Card)

Wi-Fi kartları, kablosuz ağlara bağlanmak ve kablosuz sinyalleri yakalamak için kullanılan donanımlardır. Özellikle **monitor mode** ve **packet injection** gibi özelliklere sahip kartlar, kablosuz ağ güvenlik testleri için vazgeçilmezdir.

Örnek Kullanım:

- Kablosuz ağları taramak.
- Paketleri yakalamak ve analiz etmek.
- Ağlara müdahale etmek (ör. Deauthentication saldırıları).

2. Wireshark

Wireshark, ağ trafiğini analiz etmek için kullanılan açık kaynaklı bir ağ protokol analizörüdür. Kullanıcıya ağ paketlerini detaylı bir şekilde inceleme ve çözümleme imkanı sunar.

Özellikler:

- Canlı ağ trafiği izleme.
- TCP, UDP, ICMP, DNS gibi çok sayıda protokolü analiz etme.
- Paketleri filtreleyerek belirli verileri ayıklama.
- Ağ güvenlik testlerinde ele geçirilen trafiği inceleme.

Kullanım Alanları:

- Ağ güvenliği analizi.
- Hata ayıklama.
- Veri trafiği izleme.

3. Airmon-ng

Airmon-ng, **Aircrack-ng** araç takımının bir parçasıdır ve kablosuz ağ adaptörlerini **monitor mode**a geçirme işlevi görür. Monitor mode, kablosuz ağ trafiğini pasif bir şekilde dinlemeyi sağlar.

Özellikler:

- Kablosuz kartları izleme moduna geçirme.
- Hedef ağları belirlemek için kullanılabilecek temel bir araç.
- Monitor mode'da çalışan cihazları listeleme ve durdurma.

Kullanım Alanı:

- Kablosuz trafiği dinlemek için başlangıç adımıdır.

4. Aircrack-ng

Aircrack-ng, kablosuz ağların güvenliğini test etmek için kullanılan bir araç setidir. WEP, WPA, ve WPA2 gibi şifreleme türlerini kırmaya yardımcı olur.

Özellikler:

- **Aircrack:** Şifre kırma işlemi.
- **Aireplay-ng:** Deauthentication gibi saldırılar gerçekleştirme.
- **Airmon-ng:** Monitor mode'a geçiş.
- **Airdecap-ng:** Şifrelenmiş paketleri çözümleme.

Kullanım Alanı:

- Kablosuz ağ şifreleme kırma (WEP/WPA).
- Trafik yakalama ve analiz etme.

5. Ettercap

Ettercap, ağ güvenliği testlerinde kullanılan bir **Man-in-the-Middle (MITM)** aracıdır. Yerel ağlarda trafiği izlemek, manipüle etmek ve yönlendirmek için tasarlanmıştır.

Özellikler:

- ARP Spoofing ve DNS Spoofing gibi saldırılar düzenleme.
- Şifrelenmemiş verileri yakalama.
- Hedef cihazlar arasındaki iletişimi kesintiye uğratma.

Kullanım Alanı:

- Yerel ağlardaki trafiği manipüle etme.
- Ağ tabanlı saldırılar gerçekleştirme.

6. Airgeddon

Airgeddon, kablosuz ağ penetrasyon testleri için geliştirilmiş bir **otomasyon aracıdır**. Çeşitli saldırı tekniklerini bir arada sunar ve süreçleri kolaylaştırır.

Özellikler:

- Evil Twin saldırıları yapma.
- Deauthentication saldırıları düzenleme.
- WPA/WPA2 anahtarlarını kırma.
- WPS PIN kırma.

Kullanım Alanı:

- Kablosuz ağ güvenliğini test etme.

- Sahte Wi-Fi erişim noktaları oluşturma.

7. Fluxion

Fluxion, WPA/WPA2 korumalı ağlarda sosyal mühendislik saldırıları gerçekleştirmek için kullanılan bir araçtır.

Özellikler:

- Sahte oturum açma sayfaları oluşturarak kullanıcıdan şifre alma.
- Deauthentication saldırıları düzenleyerek kullanıcıyı sahte erişim noktasına bağlama.
- Kullanıcı giriş bilgilerini gerçek zamanlı yakalama.

Kullanım Alanı:

- Sosyal mühendislik tabanlı Wi-Fi saldırıları.

8. Crunch

Crunch, güçlü bir **wordlist oluşturma aracı**dır. Şifreleme kırma veya kaba kuvvet (brute force) saldırılarında kullanılacak özel karakter setlerine göre wordlist üretir.

Özellikler:

- Özel uzunluk ve karakter setlerine göre kelime listesi oluşturma.
- Kombinasyonlar üzerinde detaylı kontrol imkanı.
- Dosya boyutuna veya içeriğe göre kısıtlamalar ayarlama.

Kullanım Alanı:

- Kablosuz ağ şifrelerini denemek için parola listesi oluşturma.
- Kaba kuvvet saldırılarında kullanılan özel diziler hazırlama

Eavesdroping

Genellikle “koklama”(sniffing) olarak adlandırılan gizli dinleme, yetkisiz bir kişinin kablosuz bir ağ üzerindeki trafiği yakaladığı ve okuduğu pasif bir saldırıdır. Esasen saldırgan, cihazlar ve ağ erişim noktaları arasında iletilen kablosuz sinyalleri “dinler”.

Nasıl çalışır?

Verilerin yakalanması: Kablosuz ağlar elektromanyetik dalgalar kullanarak veri ileterek çalıştığından, bu sinyaller uygun alıcı anten ve yazılımla donatılmış menzil içindeki herhangi bir cihaz tarafından yakalanabilir.

Kod çözme: Veriler şifrelenmemişse, bir gizli dinleyici yakalanan verileri doğrudan kolayca okuyabilir. Ancak veriler şifrelenmişse, saldırganın ele geçirilen bilgilerin kodunu çözmek ve anlamak için ek araçlara veya tekniklere ihtiyacı olacaktır.

Deauthentication attacks ve WPA/WEP Şifre Kırma

Deauth saldırılarının birkaç farklı amacı olabilir bunlardan iki tanesi şunlardır:

1. Kullancıyı ağdan düşürüp yeniden bağlanmasını sağlayarak Handshake dosyasını yakalayıp şifreyi kırmaya çalışmak

2. Evil Twin (Şeytani İkiz) saldırısı. Burda amaç ise kullanıcıyı düşürüp captive portalımıza bağlayarak wi-fi şifresini çalmak

Bu saldırının otomatikleştirilmiş hali airgeddon ile yapılaabilir manuel yapımı ise adım adım şöyle gerçekleşir.

airmon-ng check # ağı kullanan işlemleri listeler genelde 2 tane olur.
1. NetworkManager
2. wpa_suppliment

Bu çalışan işlemler ağ saldırısı esnasında sorun yaratmaması için sonlandıracağız. Bunun için kullanılacak komut;
airmon-ng check kill
airmon-ng start "IFACE" Örnek : airmon-ng start wlan0
Bu komut ile adaptörümüzü Managed modundan Monitör moduna alıyoruz. Tekrardan **iwconfig** komutu ile kontrol ediniz.

airodump-ng wlan0
monitör moduna aldığımız ağ kartı ile etrafımızda ki ağ noktalarını ve bilgilerini görüyoruz. Burada bize lazım olanlar **BSSID(modemin MAC Adresi) ,CHANNEL,ESSID** (Wi-Fi ismi) bilgileridir. Bu aşamada seçtiğiniz ağ noktasının bu bilgilerini notepade kayıt ediniz.

airodump-ng -c <HedefAğınBulunduğuKanal> --bssid <HedefModemMACAdresi> -w filename wlan0
#Bu komut ile hedef routerı dinlemeye alıyoruz bunun nedeni ise bir sonra ki aşama olan deAuth saldırısı sonrasında ağa bağlı olan kullanıcının ağa bağlanmak için gönderdiği ağ paketini yani handshke yakalamak.

aireplay-ng --deauth 10 -a modemMacAdresi -c BağlıCihazMACAdresi wlan0
Yazdığım komutu özete anlatayım. aireplay-ng kullanacağımız araç,
--deauth *parametresi ile kaç paket gönderileceğini belirtiyoruz.*
-a *parametresi ile saldırı yapılacak Router MAC Adresi giriyoruz.*
-c *parametresi ile saldırın yapılacağı (paketlerin gönderileceği) hedef cihazın MAC Adresini giriyoruz.*
ve son olarak ağ arayüzünü (interface) belirtiyoruz.

aircrack-ng -b modemMACAdresi -w wordlistadresi.txt handshake.cap

Wordlist oluşturmak için crunch kullanılabilir veya hazır wordlistler kullanabilirsiniz.

Şeytani ikiz saldırısı

Kötü İkiz Saldırısı, bir saldırganın meşru bir erişim noktasını taklit eden veya kimliğine bürünen sahte bir kablosuz erişim noktası kurmasını içerir. Bu kötü niyetli erişim noktası, meşru ağın “kötü ikizidir”. Şüphelenmeyen kullanıcılar, güvenilir veya bilinen

bir ağa bağlandıklarını düşünürken, bunun yerine saldırgan tarafından kurulan sahte erişim noktasına bağlanırlar.

Nasıl çalışır?

Kurulum: Saldırgan, genellikle “Free Airport Wi-Fi” gibi potansiyel kurbanların tanıyabileceği ortak bir ağ adı (SSID) kullanarak veya yakındaki meşru bir ağın adını kopyalayarak bir cihazı kablosuz erişim noktası olarak hareket edecek şekilde yapılandırır.

Yayınlama: Kötü ikiz erişim noktası SSID'sini yayınlayarak cihazların kendisine bağlanmasını bekler. Bazı senaryolarda saldırgan, kullanıcıların daha güçlü sinyale sahip kötü ikize bağlanma olasılığını artırmak için meşru erişim noktasına bir sinyal bozma saldırısı da düzenleyebilir.

Dinleme: Bir kullanıcı kötü ikize bağlandığında, kimlik bilgilerini ele geçirmek için sahte bir giriş sayfası sunulabilir veya saldırgan, iletilen şifrelenmemiş verileri yakalayarak çevrimiçi etkinliklerini izleyebilir.

Manipülasyon: Gelişmiş senaryolarda, saldırgan kurban tarafından gönderilen veya alınan verileri değiştirebilir veya kötü amaçlı web sitelerine yönlendirebilir.

Man-In-The-Middle Saldırıları (MITM)

Genellikle MITM olarak kısaltılan Man-In-The-Middle Saldırısı, bir saldırganın iki taraf arasındaki iletişimi gizlice yakaladığı ve aktardığı bir kablosuz ağ saldırısı biçimidir. Saldırgan, kurbanlarla bağımsız bağlantılar kurar ve aralarındaki mesajları aktararak, aslında tüm konuşma saldırgan tarafından kontrol edilirken, özel bir bağlantı üzerinden doğrudan birbirleriyle konuştuklarına inanmalarını sağlar.

Nasıl çalışır?

Dinleme: Saldırganın öncelikle kurban ile iletişim kurduğu varlık arasına girmesi gerekir (örneğin, bir kullanıcı ile bir Wi-Fi ağı arasına).

Şifre çözme (gerekirse): Ele geçirilen veri şifrelenmişse, saldırganın bu verinin şifresini çözmesi gerekir. Bu çeşitli teknikler kullanılarak yapılabilir, yaygın yöntemlerden biri kablosuz ağ senaryolarında sahte Wi-Fi erişim noktalarının kullanılmasıdır.

Aktarım ve yakalama: Saldırgan bir kaynaktan giden mesajları yakalar, potansiyel olarak değiştirir ve ardından bunları hedeflenen alıcıya gönderir. İletişimin güvenli olduğuna inanan alıcı, saldırganın tekrar yakalayabileceği, değiştirebileceği ve aktarabileceği yanıt verir.

Sonlandırma: Saldırgan istediği bilgiyi elde ettiğinde veya yeterli bozulmaya neden olduğunda, oturumu sonlandırabilir ve kurbanlar ihlalden habersiz kalabilir.

Windows Security Event ID (Kurban):

- **4647**: Kullanıcı oturumu kapandı.
  Wi-Fi bağlantısı kesilirse bu event oluşabilir.
- **4634**: Oturum kapatma.
  Kurban cihazın Wi-Fi bağlantısından düşmesi durumunda tetiklenebilir.
- **4624**: Başarılı oturum açma.
  Saldırganın kurban ağına erişim sağlaması durumunda kaydedilir.
- **5156**: İzin verilen bir bağlantı.
  Kurban cihaz ile saldırgan arasında bir ağ trafiği oluştuğunda tetiklenir.
- **4672**: Özel ayrıcalıklarla oturum açma.
  - Sahte Wi-Fi'ye bağlandıktan sonra sistem yetkileriyle ilgili etkinlikler kaydedilebilir.

Sysmon Event ID (Kurban):

- **3**: Ağ bağlantıları (Network Connection).
  - Kurban cihaz sahte Wi-Fi'ye bağlandığında kayıt yapılır.

- 22: DNS sorguları (DNS Query).
    - Sahte Wi-Fi üzerinden yapılan DNS istekleri kaydedilir.

1. Man-in-the-Middle (MITM) Saldırılarına Karşı Korunma

Teknik Yöntemler:

- **HTTPS kullanımı:**
    - Web sitelerine bağlanırken yalnızca HTTPS protokolü kullandığınızdan emin olun. Tarayıcılardaki "SSL/TLS sertifikası" hatalarına dikkat edin.
- **Güvenilir VPN kullanımı:**
    - VPN bağlantıları, MITM saldırılarında trafiğin şifrelenmesini sağlar. Güvenilir ve güçlü şifreleme kullanan VPN hizmetlerini tercih edin.
- **Ağ segmentasyonu:**
    - Kritik cihazların ve sunucuların, genel ağdan ayrı segmentlerde tutulması MITM saldırılarını zorlaştırır.
- **Static ARP tabloları kullanımı:**
    - ARP spoofing saldırılarına karşı, cihazlara statik ARP girdileri yapılandırılabilir.

Operasyonel Yöntemler:

- Ağ trafiğini düzenli olarak izleyin ve anormal aktiviteleri tespit edin.
- Yerel ağlarda yalnızca güvenilir cihazlara izin verin (MAC adres filtreleme).

2. Eavesdropping (Dinleme Saldırısı)

Teknik Yöntemler:

- **Ağ şifrelemesi:**
    - Tüm kablosuz ağlarda WPA3 gibi güçlü bir şifreleme standardı kullanın. Eski protokollerden (WEP, WPA) kaçının.
- **DNS-over-HTTPS (DoH):**
    - DNS sorgularını şifrelemek için DoH protokolünü etkinleştirin.
- **Kablosuz ağ trafiğini gizlemek:**
    - SSID yayınını devre dışı bırakmak ve MAC adres filtreleme ile yalnızca yetkili cihazların bağlanmasına izin vermek.

Operasyonel Yöntemler:

- Ortak Wi-Fi ağlarını kullanırken güvenilir bir VPN kullanın.
- Hassas işlemleri (ör. bankacılık) yaparken halka açık ağlardan uzak durun.

3. Evil Twin (Sahte Erişim Noktası)

Teknik Yöntemler:

- **Karmaşık şifreler:**
  - Wi-Fi ağlarınız için güçlü ve karmaşık şifreler belirleyin.
- **Kablosuz istemci izolasyonu:**
  - Ağınızdaki cihazlar arasında doğrudan iletişimi engelleyen özellikleri etkinleştirin.
- **Güvenli erişim kontrolü:**
  - WPS özelliğini devre dışı bırakın ve yalnızca WPA2/WPA3 protokollerini kullanın.

Operasyonel Yöntemler:

- Bağlandığınız Wi-Fi ağlarının ismini ve doğruluğunu kontrol edin.
- Şüpheli Wi-Fi ağlarına bağlanmaktan kaçının.

4. WEP/WPA Key Cracking (Şifre Kırma)

Teknik Yöntemler:

- **WPA3 kullanımı:**
  - Güvenlik protokolü olarak WPA3 kullanın. WPA ve özellikle WEP protokollerinden uzak durun.
- **Güçlü parolalar belirleyin:**
  - Karmaşık ve uzun Wi-Fi şifreleri kullanarak saldırganların parola kırma işlemlerini zorlaştırın.

Operasyonel Yöntemler:

- Düzenli aralıklarla Wi-Fi şifrelerini değiştirin.
- Wi-Fi ağına bağlı cihazları düzenli olarak kontrol edin.

5. Deauthentication Saldırıları

Teknik Yöntemler:

- **802.11w standardını etkinleştirin:**
  - Bu özellik, yönetim çerçevelerini şifreleyerek deauthentication saldırılarını etkisiz hale getirir.
- **Erişim kontrol listesi (ACL):**
  - Ağa yalnızca belirli MAC adreslerinin bağlanmasına izin veren bir ACL yapılandırın.

Operasyonel Yöntemler:

- Wi-Fi ağına bağlı cihazların bağlantı kesilmesi gibi anormal durumları izleyin.
- Ağ trafiğini düzenli olarak denetleyerek anormal davranışları analiz edin.

Genel Korunma Stratejileri

- **Ağ İzleme Araçları Kullanımı:**
  - Sysmon, Wazuh veya diğer SIEM araçlarıyla ağ trafiği ve cihaz etkinliklerini sürekli izleyin.
- **Eğitim:**
  - Kullanıcıları sahte ağlar ve MITM saldırıları hakkında bilinçlendirin.
- **Güncelleme ve Yama:**
  - Tüm cihazlar ve ağ ekipmanları için en son yazılım güncellemelerini ve güvenlik yamalarını uygulayın.
- **Firewall ve IDS/IPS:**
  - Ağınıza gelen ve ağdan çıkan trafiği izlemek ve şüpheli aktiviteleri engellemek için güvenlik duvarları ve izinsiz giriş tespit/önleme sistemlerini etkinleştirin.

Deauth saldıralarında modemlerde sürekli paket göderildiğinde modemler paket gönderen IP yı yasaklayabiliyor. Böyle saldırıları açık alanda (kafe, havaalanı) gibi yerlerde denemeyin çoktan yapılandırılması yapılmış olabilir.

SSH Bruteforce

SSH (Secure Shell), uzak sunuculara güvenli bir şekilde bağlanmak için kullanılan bir protokoldür. **SSH Brute Force saldırısı**, saldırganın bir SSH sunucusuna erişim sağlamak amacıyla sistematik bir şekilde farklı kullanıcı adı ve parola kombinasyonlarını deneyerek doğru kimlik bilgilerini tahmin etmeye çalıştığı bir saldırı türüdür.

Kullanılan araç/toolslar:

Hydra, hızlı ve esnek bir brute force aracı olup farklı protokoller için destek sunar. Özellikle ağ protokolleri ve uzak hizmetler üzerinde oturum açma kimlik bilgilerini test etmek için yaygın olarak kullanılır.

Özellikler:

1. **Desteklenen Protokoller:**
    a. SSH, FTP, HTTP, RDP, SMB, Telnet, SNMP, VNC, MySQL, PostgreSQL, Oracle, LDAP, ve daha fazlası.
2. **Hızlı ve Esnek:**
    a. Birden fazla parola denemesini eşzamanlı olarak yapabilir (çok iş parçacıklı).
3. **Komut Satırı Tabanlı:**
    a. Terminal üzerinden çalışır ve kolayca özelleştirilebilir.
4. **Parola Listesi Kullanımı:**
    a. Kullanıcı adı ve parola listelerini test etmek için dosyaları kullanır (örneğin, `rockyou.txt`).
5. **Modüler Yapı:**
    a. Yeni protokoller için modüller eklenebilir.

Kullanım Örneği:

- SSH üzerinde brute force saldırısı:

```
bash
Kodu kopyala
hydra -l root -P /path/to/passwords.txt ssh://192.168.1.10
```

    - `-l`: Tek bir kullanıcı adı (örneğin, "root").
    - `-P`: Parola listesi.
    - `ssh://`: Test edilecek protokol ve hedef IP adresi.

Avantajlar:

- Çok sayıda protokol desteği.
- Kolay yapılandırma ve kullanım.
- Hızlı ve çok iş parçacıklı saldırılar.

Kısıtlamalar:

- Ağ güvenlik önlemleri (ör. hız sınırlama, Fail2Ban) karşısında etkisiz kalabilir.
- Deneme sayısı yüksek olduğunda tespit edilme riski artar.

Medusa, Hydra'ya benzer şekilde çalışan bir brute force aracıdır, ancak genellikle daha hafif ve hızlı bir alternatif olarak tercih edilir. Yüksek eşzamanlılık (concurrency) yetenekleri sayesinde büyük kullanıcı/parola kombinasyonları üzerinde etkili bir şekilde çalışır.

Özellikler:

1. **Desteklenen Protokoller:**
    a. SSH, FTP, HTTP, Telnet, VNC, SMTP, POP3, IMAP, MySQL, MSSQL, RDP, ve diğer popüler protokoller.
2. **Esneklik ve Özelleştirilebilirlik:**
    a. Test edilen kullanıcı adı ve parola çiftlerini kolayca özelleştirme imkanı.
3. **Hafif ve Verimli:**
    a. Sistem kaynaklarını az tüketir ve paralel işlemleri optimize eder.
4. **Doğrudan Hizmet Tespiti:**
    a. Belirli bir hizmeti tarayarak hedef protokolü algılayabilir.

Kullanım Örneği:

- SSH brute force saldırısı:

```
bash
Kodu kopyala
medusa -h 192.168.1.10 -u root -P /path/to/passwords.txt -M ssh
```

    - `-h`: Hedef IP adresi.
    - `-u`: Tek bir kullanıcı adı (örneğin, "root").
    - `-P`: Parola listesi.
    - `-M`: Modül (protokol) seçimi.

Avantajlar:

- Yüksek eşzamanlılık sayesinde büyük parola listelerini hızlı bir şekilde test edebilir.
- Modüler yapısı yeni hizmetler eklemek için uygundur.
- Performansı optimize edilmiş bir yapıdadır.

Kısıtlamalar:

- Daha az protokol desteği (Hydra'ya kıyasla).
- Saldırılar sırasında ağ güvenlik önlemleri tarafından engellenebilir.

Kurban Makinede Windows Security Event ID'leri

1. **Event ID 4625 - Failed Logon (Başarısız Giriş Denemesi)**
    a. Yanlış kullanıcı adı veya parola ile giriş yapılmaya çalışıldığında tetiklenir.
    b. Brute force saldırısının en belirgin göstergesidir.
    c. Önemli Alanlar:
        i. *Logon Type:* (Logon Türü)
            1. **3:** Ağdan giriş denemesi (ör. SMB, RDP).
            2. **10:** Uzak masaüstü oturumu (RDP).
        ii. *Account Name:* Hedef kullanıcı adı.
        iii. *Source IP Address:* Saldırının kaynağı.
    d. Örnek:

```
yaml
Kodu kopyala
An account failed to log on.
Logon Type: 3
Account Name: admin
Source Network Address: 192.168.1.100
```

2. **Event ID 4771 - Kerberos Authentication Ticket Failure**
    a. Yanlış parola ile Kerberos tabanlı kimlik doğrulama başarısız olduğunda tetiklenir.
    b. Özellikle Active Directory ortamlarında saldırıyı tespit etmek için önemlidir.
    c. "Pre-authentication failed" hatası içerir.
3. **Event ID 4624 - Successful Logon (Başarılı Giriş)**
    a. Eğer saldırgan doğru kullanıcı adı ve parolayı bulursa başarılı giriş kaydı oluşur.

   b. Hangi oturum türüyle giriş yapıldığını kontrol edin (ör. RDP için **Logon Type 10**).
4. **Event ID 4768 - Kerberos Authentication Ticket Granted**
   a. Saldırgan doğru parolayı bulduğunda Kerberos bileti başarıyla alınır.

Kurban Makinede Sysmon Event ID'leri

1. **Event ID 3 - Network Connection Detected**
   a. Brute force sırasında kurban makinenin hedef protokol portuna gelen sürekli bağlantı taleplerini loglar.
   b. Örneğin:
      i. SSH brute force: Port **22**.
      ii. RDP brute force: Port **3389**.
      iii. SMB brute force: Port **445**.
   c. Log Örneği:

```
yaml
Kodu kopyala
Network connection detected:
Source IP: 192.168.1.100
Destination IP: 192.168.1.10
Destination Port: 3389
```

2. **Event ID 1 - Process Creation**
   a. Brute force saldırısının hedefi olan sistemde kullanıcı oturum açtığında, ilgili oturumu başlatan işlemler loglanır.
   b. Örneğin, doğru kimlik bilgileriyle giriş yapıldığında **mstsc.exe** (RDP bağlantı işlemi) başlar.
3. **Event ID 10 - Process Access**
   a. Bir kullanıcı veya hizmet (ör. SMB) başarısız giriş denemelerinde kurban sistemindeki işlemlere erişim talep edebilir.

PowerShell Event ID'leri

PowerShell tabanlı brute force araçları kullanılıyorsa, kurban sisteminde PowerShell ile ilgili event ID’ler tetiklenebilir:

1. **Event ID 4104 - Script Block Logging**
   a. Eğer saldırgan PowerShell üzerinden brute force denemesi yapıyorsa, ilgili komutlar veya script blokları loglanır.

b. Örnek:

```
powershell
Kodu kopyala
Invoke-BruteForce -Target 192.168.1.10 -Port 22 -User admin -
PassList passwords.txt
```

2. **Event ID 4103 - PowerShell Pipeline Execution**
    a. Bir PowerShell komutunun yürütülmesi sırasında tetiklenir.
3. **Event ID 4688 - Process Creation (PowerShell ile Başlatılan İşlem)**
    a. PowerShell tabanlı bir brute force saldırısında ilgili işlemin çalıştırıldığı kaydedilir.

Korunma Yöntemleri

1. Parola Politikaları ve Güvenliği

1. **Güçlü Parolalar Kullanın:**
    a. Parolalar en az **12 karakter uzunluğunda**, harf (büyük/küçük), rakam ve özel karakter içermelidir.
    b. Tahmin edilmesi zor, rastgele oluşturulmuş parolalar kullanılmalıdır.
2. **Parola Denemesi Sınırı:**
    a. Bir kullanıcı için belirli sayıda başarısız giriş denemesinden sonra hesabı geçici olarak kilitleyin.
    b. Windows: **Hesap Kilitlenme Eşiği** ayarı.
    c. Linux: `/etc/pam.d/common-auth` üzerinden ayar yapabilirsiniz.
3. **Parola Yönetimi:**
    a. Parolaları düzenli aralıklarla değiştirin.
    b. Her hesap için farklı bir parola kullanın.

2. İki Faktörlü Kimlik Doğrulama (2FA)

- **Ekstra Güvenlik Katmanı:**
    - Kullanıcı adı ve parola ile birlikte ikinci bir doğrulama yöntemi (ör. telefon uygulaması, SMS, biyometrik) kullanın.
    - SSH için Google Authenticator veya Duo gibi araçları entegre edebilirsiniz.
    - RDP bağlantılarında 2FA sağlayan çözümler kullanabilirsiniz.

3. Giriş Denemelerini Sınırlama

1. **SSH İçin:**
    a. **Fail2Ban veya SSH Guard:** Belirli sayıda başarısız giriş denemesinden sonra saldırganın IP adresini geçici olarak engeller.
        i. Kurulum (Debian/Ubuntu):

```
bash
Kodu kopyala
sudo apt install fail2ban
```

2. **Windows için Hesap Kilitlenme Politikası:**
    a. **Yerel Güvenlik Politikası > Hesap Politikaları > Hesap Kilitleme Eşiği** üzerinden giriş sınırı belirleyebilirsiniz.
3. **Firewall Ayarları:**
    a. Sadece güvenilir IP'lerin girişine izin verin.
    b. SSH bağlantılarını sadece güvenilir bir IP aralığı ile sınırlayın:

```
bash
Kodu kopyala
sudo ufw allow from <trusted-ip> to any port 22
```

4. Uygulama ve Protokol Ayarları

1. **SSH Güvenliği:**
    a. **Varsayılan Portu Değiştirin:** SSH bağlantı portunu (22) farklı bir port numarasına taşıyın:

```
bash
Kodu kopyala
sudo nano /etc/ssh/sshd_config
Port 2222
```

    b. **Kök Kullanıcı Girişini Devre Dışı Bırakın:**

```
perl
Kodu kopyala
PermitRootLogin no
```

    c. **Sadece SSH Anahtarlarını Kabul Edin:** Parola doğrulaması yerine yalnızca SSH anahtarları ile girişe izin verin.

4. SIEM Kullanmak

Örnek olarak size smbd bruteforce tespiti için yazdığım bir wazuh kuralını göstereceğim. Bunun ilk önce ossec.conf dosyasına logların kaydedildiği yolu eklemeniz gerekiyor.

/var/log/auth.log

Ekledikten sonra yapmanız gereken şey başarısız bir giriş yapma denemesinde çıkan logta yazılan kaydı öğrenmeniz gerekiyor. Birazdan neden olduğunu anlatacağım.

Failed password for invalid user admin from <IP> port 22 ssh2

```
<group name="smbd">
  <rule id="100004" level="5">
    <match>NT_STATUS_WRONG_PASSWORD</match>
    <description>SMBD GİRİŞ DENEMESİ!</description>
    <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,gpg13_7.8,gdpr_IV_35.7.d,
    gdpr_IV_32.2,hipaa_164.312.b,nist_800_53_AU.14,nist_800_53_AC.7,tsc_CC6.1,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,</group>
  </rule>

  <rule id="100009" level="8" frequency="5" timeframe="30">
    <if_matched_sid>100004</if_matched_sid>
    <description>SMBD BRUTE FORCE!</description>
    <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,gpg13_7.8,gdpr_IV_35.7.d,
    gdpr_IV_32.2,hipaa_164.312.b,nist_800_53_AU.14,nist_800_53_AC.7,tsc_CC6.1,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,</group>
  </rule>
</group>
```

Burada sadece yukarıdaki sshd.*Failed password kısmını match kısmına eklemeniz gerekiyor. Yukarıdaki şeylerin anlamlarını aşağı yazacağım smb yerine ssh olarak düşünün çalışma mantığı aynı.

1. `<group name="smbd">`

- **Açıklama:** Bu, Wazuh kural setinde belirli bir protokol veya olay grubu için tanımlanan bir grup adıdır. Burada, **"smbd"**, SMB protokolüne yönelik olayların işlenmesi için oluşturulmuş bir grup adıdır.
- **Amacı:** Aynı protokole veya türdeki olaylara ait kuralları bir arada gruplamak için kullanılır.

2. `<rule id="100004" level="5">`

- **`id="100004"`:** Bu, Wazuh tarafından kullanılan kuralın benzersiz kimliğidir. Her kuralın bir ID'si vardır ve bu ID, log dosyasında tetiklenen kuralı tanımlamak için kullanılır.
- **`level="5"`:** Bu, olayın önem derecesini belirtir. Wazuh'da seviye **0-15** arasında bir değer alır:
    - **5:** Orta düzeyde bir tehdit veya bilgi olayıdır. Bu seviyede olay, kullanıcı dikkati gerektirir, ancak acil değildir.

3. `<match>NT_STATUS_WRONG_PASSWORD</match>`

- **Açıklama:** Bu, log dosyasındaki belirli bir ifadeyi yakalamak için kullanılan bir eşleştirme parametresidir.
- **`NT_STATUS_WRONG_PASSWORD`:** SMB üzerinden yanlış bir parola ile kimlik doğrulama denemesi yapıldığını ifade eder.
- **Amacı:** Yanlış parolalı giriş denemelerini algılamak için bu ifadeye sahip logları kontrol eder.

4. `<description>SMBD GİRİŞ DENEMESİ!</description>`

- **Açıklama:** Kural tetiklendiğinde oluşturulacak açıklamadır. Burada, SMB protokolü üzerinden başarısız giriş denemelerinin bir göstergesi olarak tanımlanmıştır.

5. `<group>` (İç Gruplar)

- **Açıklama:** Kuralın hangi güvenlik standartlarıyla ilişkilendirildiğini veya ne tür bir olay olduğunu tanımlar.
- **Örnek:**
    - **`authentication_failed`:** Kimlik doğrulama hatası.
    - **`pci_dss_10.2.4`:** PCI DSS güvenlik standardına göre, başarısız oturum açma denemelerinin loglanması gerektiğini ifade eder.
    - **`nist_800_53_AC.7`:** NIST güvenlik standardına göre kimlik doğrulama mekanizmalarının izlenmesi gerektiğini belirtir.
    - **`gdpr_IV_32.2`:** GDPR'nin ilgili kısmıyla uyumluluk sağlar.

6. `<rule id="100009" level="8" frequency="5" timeframe="30">`

- **`id="100009"`:** Benzersiz kural kimliği.
- **`level="8"`:** Daha yüksek bir tehdit seviyesi. **8**, genellikle önemli veya kritik bir olay anlamına gelir.
- **`frequency="5"`:** Bu kural, belirli bir süre içinde (örneğin **5 giriş denemesi**) tetiklenirse devreye girer.
- **`timeframe="30"`:** Belirtilen **30 saniye** içinde olayın meydana gelmesi gerektiğini ifade eder.

7. `<if_matched_sid>100004</if_matched_sid>`

- **Açıklama:** Bu, başka bir kuralın (ör. **id=100004**) tetiklenmiş olmasını şart koşar.
- **Amacı:** Önceki kurallara bağlı tetiklenme koşulları oluşturmak. Bu durumda, **100004** kuralı tetiklenmişse bu kural çalışır.

8. `<description>SMBD BRUTE FORCE!</description>`

- **Açıklama:** Kural tetiklendiğinde oluşturulacak açıklamadır. Burada, SMB üzerinden yapılan **brute force saldırısı** tespiti ifade edilmiştir.

9. Diğer Etiketler ve Alanlar

- **`level="8"`:** Daha yüksek bir tehdit seviyesi belirtir. Brute force saldırıları, genellikle daha ciddi bir güvenlik riski olarak değerlendirilir.
- **`frequency` ve `timeframe`:** Belirli bir süre içinde tekrarlayan olayların tespitini sağlar. Örneğin, 30 saniyede 5 başarısız giriş denemesi yapılırsa bu kural tetiklenir.