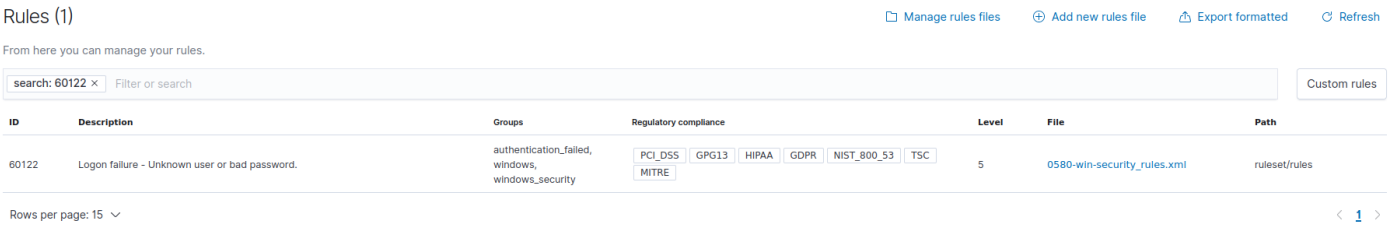
Wazuh için Custom Rule

Amaç

Unknown user or bad password. 5 dakikada aynı kullanıcı adı ve şifre için bu hatayı alıyorsak bunu bir mail ile ilgililere bildirmek.

Ad?mlar

1. EventID ile ilişkili Rule'u bulmaca (rule'un yanında 0580-win-security_rules.xml 'e bak RuleID=60122)



2. Bu Rule'u notepad veya benzeri bir alana kopyala
3. /var/ossec/ruleset/rules/0580-win-security_rules.xml dosyasını aç. 60122 ID li kuralı bul.

Nano ile ^w kullanabilirsiniz.

```
  <rule id="60122" level="5">
  <if_sid>60105</if_sid>
  <field name="win.system.eventID">^529$|^4625$</field>
  <options>no_full_log</options>
  <description>Logon failure - Unknown user or bad password.</description>
  <mitre>
    <id>T1078</id>
    <id>T1531</id>
  </mitre>

<group>authentication_failed,gdpr_IV_32.2,gdpr_IV_35.7.d,gpg13_7.1,hipaa_164.312.b,nist_800_53
_AC.7,nist_800_53_AU.14,pci_dss_10.2.4,pci_dss_10.2.5,tsc_CC6.1,tsc_CC6.8,tsc_CC7.2,tsc_CC$
</rule>
```

4. Custom Rule'ların ID leri 100.000 ile 120.000 arası olması gerekiyor. Bu nedenle 3 ncü adımda kopyaladığımız Rule da ID yi değiştir. Örn=1000001 yap.
   Aşağıdaki gibi olmalıdır

```
 <group name="custom rules">
 <rule id="100001" frequency="2" timeframe="300" level="10" overwrite="yes">
 <if_sid>60105</if_sid>
 <field name="win.system.eventID">^529$|^4625$</field>
 <options>no_full_log</options>
 <description>Logon failure - Unknown user or bad password(HM).</description>
 <mitre>
   <id>T1078</id>
   <id>T1531</id>
 </mitre>

<group>authentication_failed,gdpr_IV_32.2,gdpr_IV_35.7.d,gpg13_7.1,hipaa_164.312.b,ni
st_800_53_AC.7,nist_800_53_AU.14,pci_dss_10.2.4,pci_dss_10.2.5,tsc_CC6.1,tsc_CC6.8,ts
c_CC7.2,tsc_CC$
 </rule>
</group>
```

   Not: Rule Id satırındaki frequncy (300 saniye de 2 kez olursa) ve level parametrelerini eklemeyi unutma!!!
5. wazuhu yeniden başlat.

```
 sudo systemctl restart wazuh-manager
```

Revision #2
Created 2023-02-11 14:21:24 UTC by Hüseyin Günaydın
Updated 2023-02-11 14:55:28 UTC by Hüseyin Günaydın