

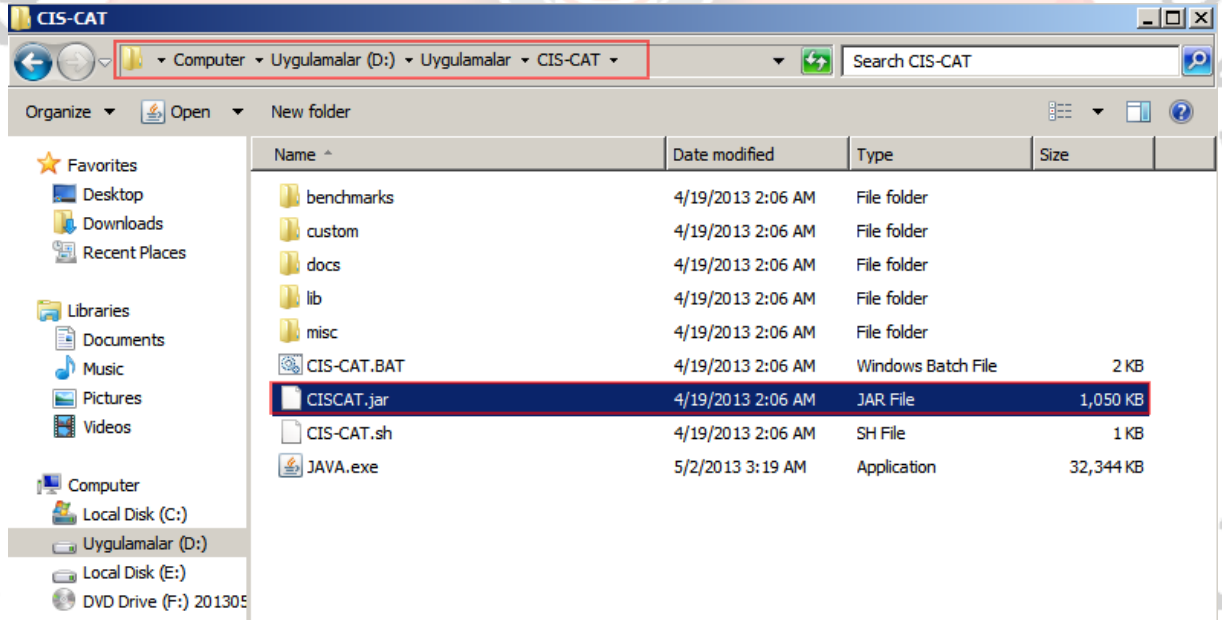
## Uygulama 5- Cis - Cat

### Önbilgilendirme

- Bu uygulama etki alanı denetleyicisi (WGE-PC) ve istemci üzerinde gerçekleştirilecektir.
- Bu uygulama, etki alanı denetleyicisi üzerinde Administrator, istemci üzerinde Yerel Yönetici kullanıcısı oturumu açıkken gerçekleştirilecektir.

### CIS-CAT ile Tarama

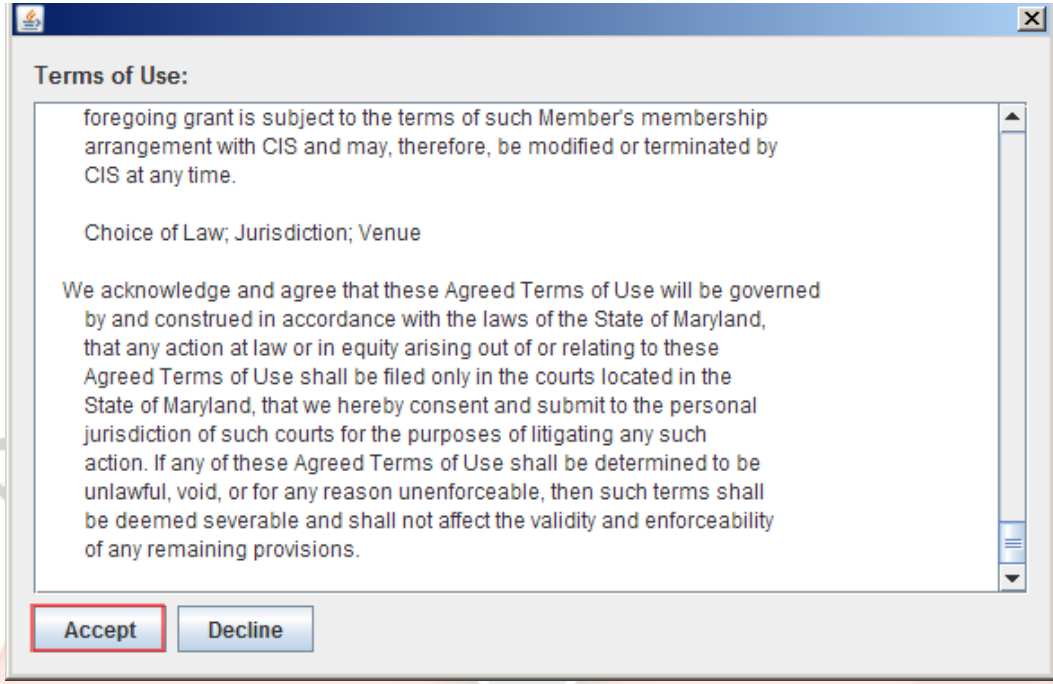
D:\Uygulamalar\CIS-CAT klasörü altındaki CIS-CAT.BAT betiği başlatılır.



Şekil - 1: CIS-CAT Uygulamasının Başlatılması

**Not:** Java yüklü değilse, aynı klasör içerisindeki JAVA.exe kullanılarak yükleme işlemi gerçekleştirilir.

Gelen kullanım sözleşmesi kabul edilir.



Şekil - 2: Kullanım Sözleşmesinin Kabul Edilmesi

Denetimi yapılacak işletim sistemi seçilir.



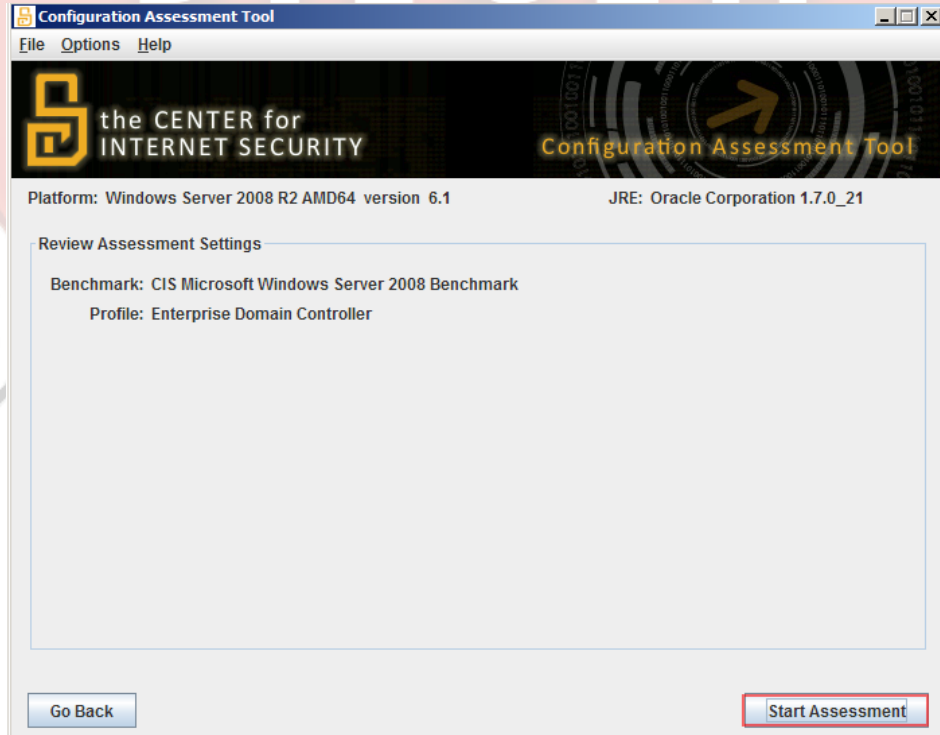
Şekil - 3: Denetlenecek İşletim Sisteminin Belirtilmesi

Profil seçimi gerçekleştirilir.



Şekil - 4: Denetim Profiline Belirtilmesi

Denetim başlatılır.



Şekil - 5: Denetimin Başlatılması

Tarama işlemi tamamlanmasıyla sonraki adıma geçilir.



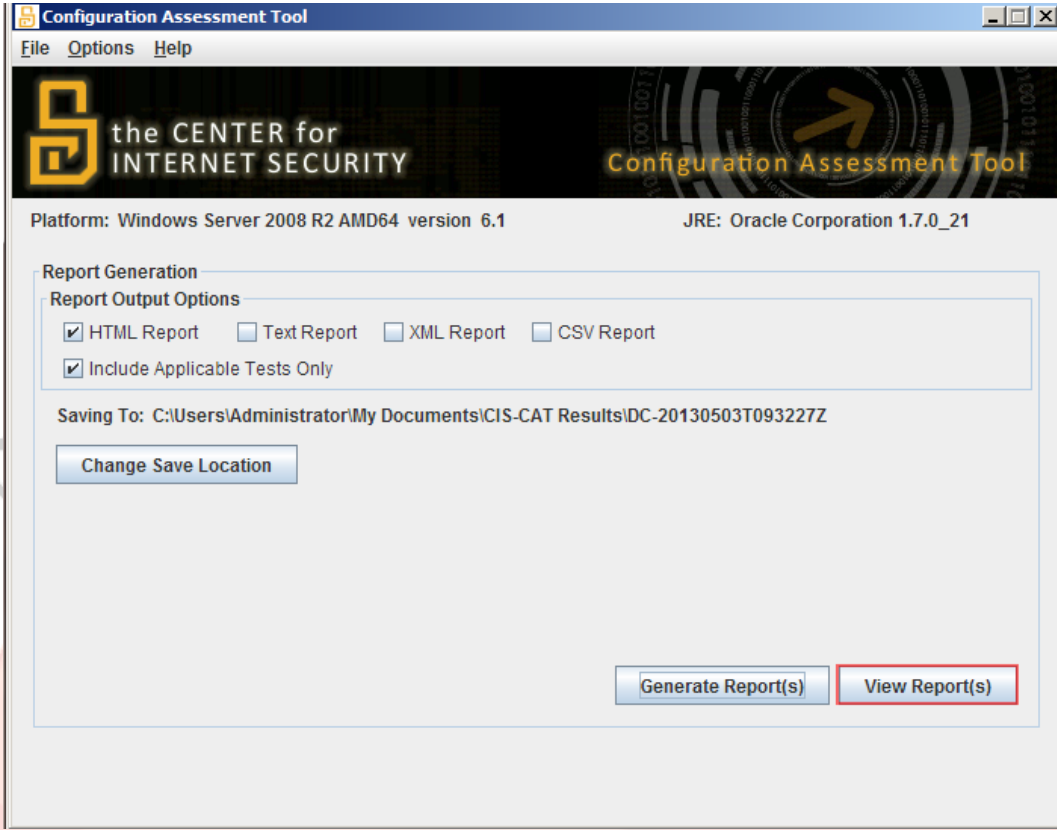
Şekil - 6: Tarama İşleminin Gerçekleşmesi

Denetim sonucunda istenilen formatta rapor oluşturulabilir.



Şekil - 7: Tarama Sonuç Raporunun Oluşturulması

İster ara yüzden ister raporun kaydedildiği dizine gidilerek rapor sonucu incelenebilir.



Şekil - 8: Raporun Görüntülenmesi - 1

HTML formatındaki rapor aşağıdaki gibidir.

**BİLGEM**

**SİBER GÜVENLİK  
ENSTİTÜSÜ**

Benchmark Result cis\_microsoft\_windows\_2008\_server\_benchmark-result-20130503093228Z - Windows Internet Expl...

C:\Users\Administrator\My Documents\CIS-CAT Results\DC

Bing

Favorite Suggested Sites Web Slice Gallery

Benchmark Result cis\_microsoft\_windows\_2008\_serv...

Page Safety Tools

### Assessment Results

Benchmark Item	Result
<b>1 Recommendations</b>	
<b>1.1 Account Policies</b>	
10.0 1.1.1 Enforce password history	Pass
10.0 1.1.2 Maximum Password Age	Pass
10.0 1.1.3 Minimum password age	Pass
10.0 1.1.4 Minimum password length	Fail
10.0 1.1.5 Password must meet complexity requirements	Pass
10.0 1.1.6 Store passwords using reversible encryption	Pass
10.0 1.1.7 Account lockout duration	Pass
10.0 1.1.8 Account lockout threshold	Pass
10.0 1.1.9 Reset account lockout counter after	Pass
10.0 1.1.10 Enforce user logon restrictions	Fail
10.0 1.1.11 Maximum tolerance for computer clock synchronization	Pass
10.0 1.1.12 Maximum lifetime for service ticket	Pass
10.0 1.1.13 Maximum lifetime for user ticket renewal	Pass
10.0 1.1.14 Maximum lifetime for user ticket	Pass
<b>1.2 Audit Policies</b>	
10.0 1.2.10 Audit: Shut down system immediately if unable to log security audits	Pass
10.0 1.2.11 Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Fail
<b>1.3 Detailed Audit Policy</b>	
10.0 1.3.1 Audit Policy: System: IPsec Driver	Fail
10.0 1.3.2 Audit Policy: System: Security State Change	Fail
10.0 1.3.3 Audit Policy: System: Security System Extension	Fail
10.0 1.3.4 Audit Policy: System: System Integrity	Pass
10.0 1.3.5 Audit Policy: Logon-Logoff: Logoff	Pass
10.0 1.3.6 Audit Policy: Logon-Logoff: Logon	Fail
10.0 1.3.7 Audit Policy: Logon-Logoff: Special Logon	Pass
10.0 1.3.8 Audit Policy: Object Access: File System	Pass
10.0 1.3.9 Audit Policy: Object Access: Registry	Pass
10.0 1.3.10 Audit Policy: Privilege Use: Sensitive Privilege Use	Pass
10.0 1.3.11 Audit Policy: Detailed Tracking: Process Creation	Fail
10.0 1.3.12 Audit Policy: Policy Change: Audit Policy Change	Fail

Done Computer Protected Mode: Off 75%

Şekil - 9: Raporun Görüntülenmesi - 2