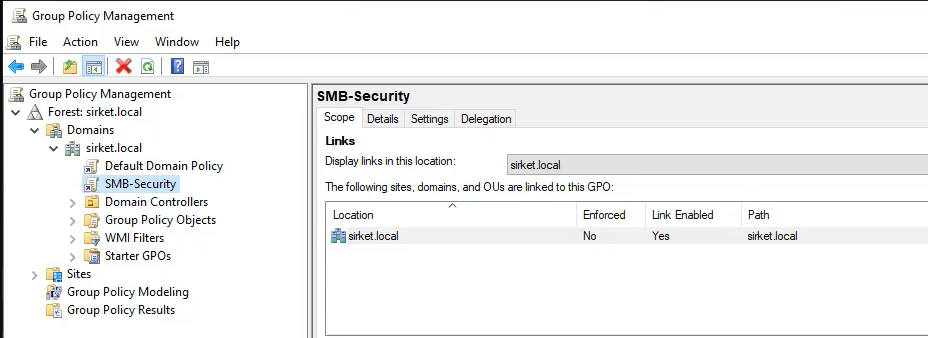
|  |
| --- |
| ***Server Security*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| Server üzerine gerçekleştirdiğim saldırıları nasıl engelleyebileceğimi ve daha güvenilir hale getirmek için hangi kuralları ekleyeceğimi göstereceğim. |

**07.02.2022**

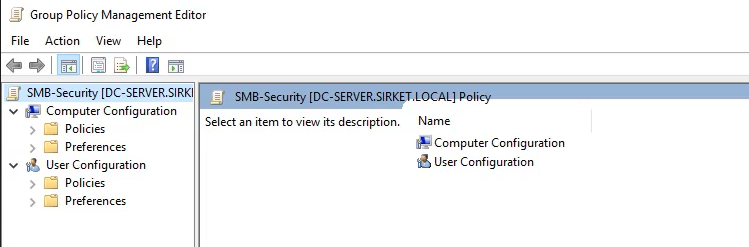
***SMB Güvenliği***

-SMB Servisi üzerinde açık kullanarak erişim sağladığımızı biliyoruz.

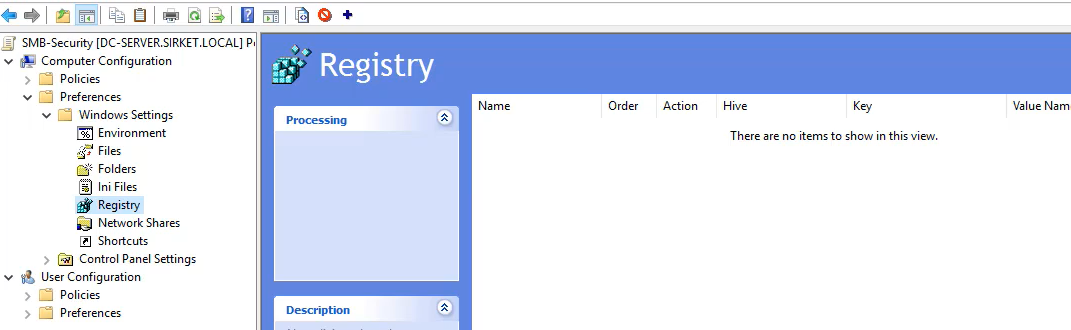
-Oluşturduğum Server üzerinde bulunan "Group Policy Management" üzerinde kurallar ekleyerek bu açıkları kapatmaya çalışacağım.



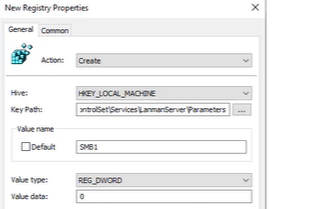
- "Group Policy Management" üzerinde "SMB-Security" isimli bir kural oluşturuyorum.



- Ardından kurala sağ tıklayıp "Edit" butonu ile içeriğine geçiş yapıyorum.

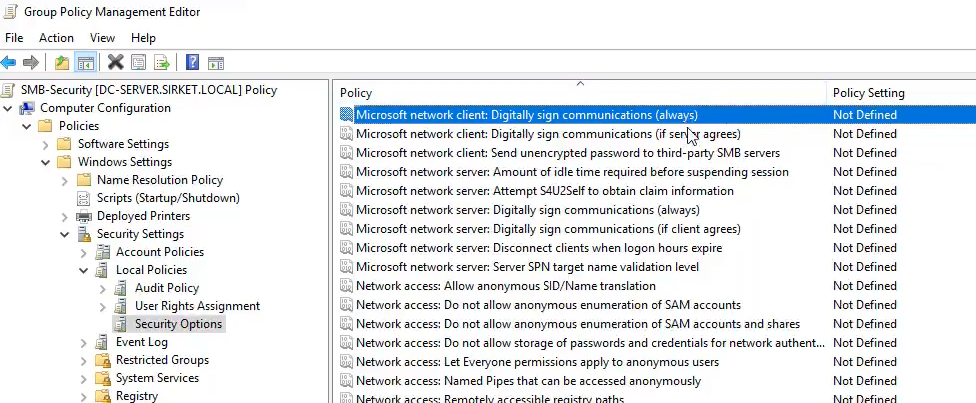


- "Prefences>WindowsSettings>Registry" içerisine geçiş yapıyorum.

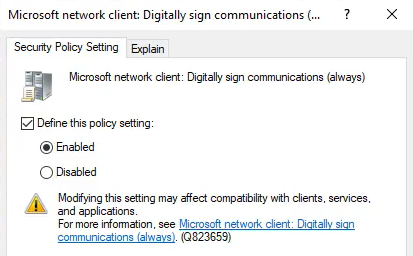


- Burada yeni bir özellik tanımlıyorum.Belirttiğim yol üzerinde ki servisi devre dışı bırakıyorum.

-Bu özellik ile SMBv1 devre dışı bırakılacaktır.



Ayrıca "SMB Security" üzerine tekrardan geçiş yapıyorum.



-Burada bulunan "Digitally Sign Communication" ayarını Enable hale getiriyorum.

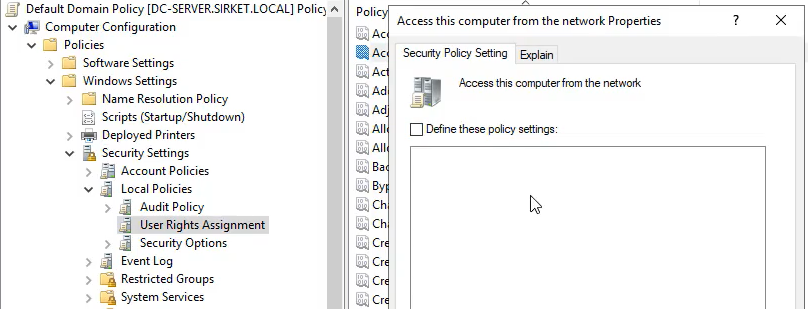
-SMB Signing kullanarak iletişim kurmasını aktif ediyorum.

***Networkten Erişimlerin Kısıtlanması***

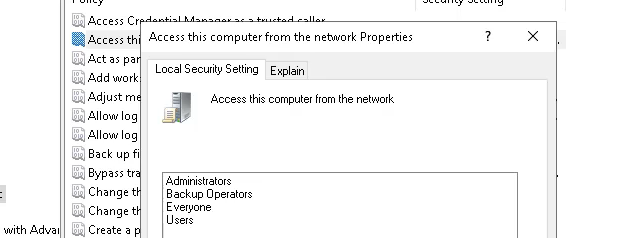
-Server üzerinde Network üzerinden Erişimlerin kısıtlanmasını istiyorsak;

-Domain control için sağlıklı bir ayar olmayacaktır.Bu ayarı kısıtlamak server için çok mantıklı olmaz.

-Local PC'ler üzerinde işlem yapılabilir.



- Server üzerinde "WindowsSet>SecuritySet>UserRightsAssigment" içerisinde bulunan "Access the computer from the network" kurala ekleyeceğimiz kullanıcılar ile sadece belirttiğimiz kullanıcılara erişim verebiliriz.

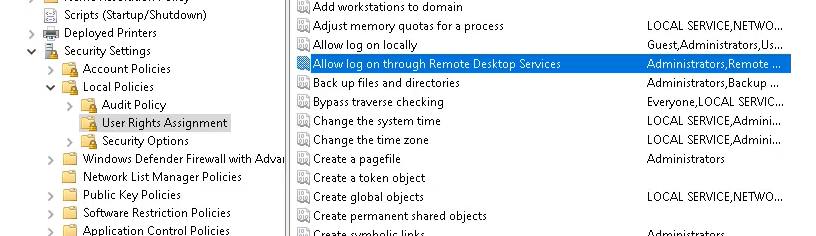


- Local üzerine geçiş yaptığımda "WindowsSet>SecuritySet>LocalPolicies>UserRightsAssigment" içerisinde bulunan yine aynı kural ile erişim sağlayabilecek kullanıcıları görüntüleyebiliyoruz.

-Eğer bu bilgisayar özel bir bilgisayar herkesin erişmemesi gerekiyorsa admin harici kullanıcılar silinebilir.

***RDP Erişimlerinin Kısıtlanması***

-Sızma işlemlerinde sıkça kullandığım RDP servisini devre dışı bırakacağım.

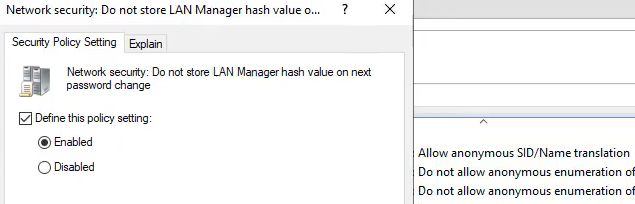


- Local üzerinde "WindowsSet>SecuritySet>UserRightsAssigment" içerisinde bulunan "RemoteDesktopServices" ayarını kullanarak uzaktan erişim üzerinde yetkilendirme yapılabilir.

-Bu kuralı Server üzerinde değiştirirsem tüm clientler üzerinde aynı ayar işlenir.

***LM Hashlerinin Kapatılması***

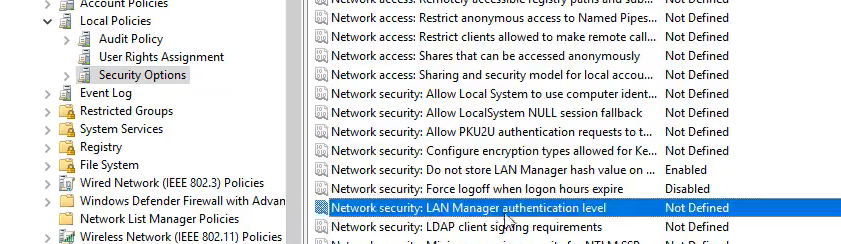
-Disk üzerinde depolanan LM Hashlerini PTH saldırıları sırasında görmüştük.



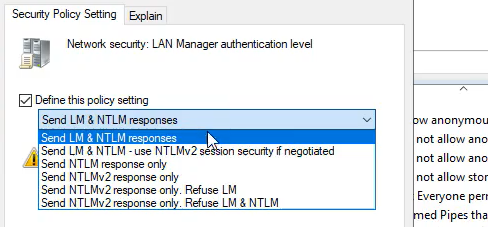
-Local üzerinde "WindowsSet>SecuritySet>LocalPolicies>SecurityOpt" içerisinde bulunan "Do Not Store Lan Manager Hash Value" kuralını devre dışı bırakarak depolanmasını engelleyebiliriz.

***NTLMv1 Kullanımının kapatılması***

-NTLM Hashlerini kullanarak PTH saldırı gerçekleştirmiştik bu hashleri şifreleme seviyesini değiştirerek erişimi az da olsa engelleyebiliriz.



-Local üzerinde "WindowsSet>SecuritySet>LocalPolicies>SecurityOpt" içerisinde bulunan "LAN Manager Auth.Lv." komutu ile hash seviyesini değiştirebilirim.

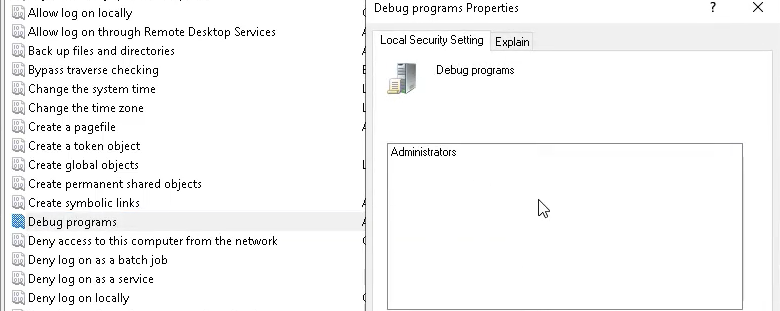


-Seviye değerlerini buradan görüntüleyebiliriz.

-Server'a uygun olanı burada belirtebiliriz.

***Debug hakkının kaldırılması***

-Kullanıcılar üzerinde bulunan Debug hakkının kaldırılması da güvenlik açısından önemlidir.



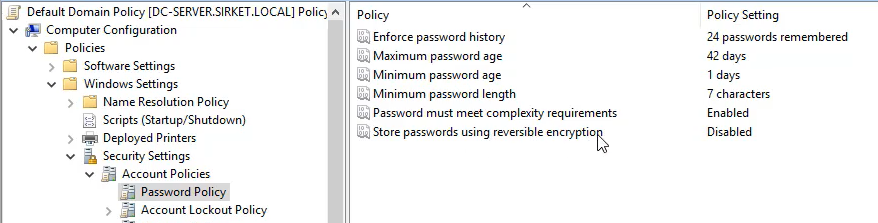
-Local üzerinde "WindowsSet>SecuritySet>LocalPolicies>UserRightsAsssig." içerisinde bulunan "Debug programs properties" kuralı içerisinde yapacağımız değişiklik ile erişimleri kapatılabilir.

-Server üzerinde kullandığımız uygulamaların etkilenip etkilenmeyeceğini göz önünde bulundurmalıyız.

-Local üzerinde gözümüz kapalı kapatabiliriz.

***Parola Güvenliği***

-"PasswordPolicy" üzerinde de güvenlik arttırmakta kesinlikle fayda vardır.



-Local üzerinde "WindowsSet>SecuritySet>PasswdPolicy" içerisinde özellikle "StorePassword" ayarının disable hale getirilmesi gerekmektedir.

-Şifrelenmiş bir şekilde depolanan şifreler çözülüp kullanılabilir.

-Ayrıca "Complexity" seçeneğini "Enable" haline getirip komplex hale getirilmelidir.

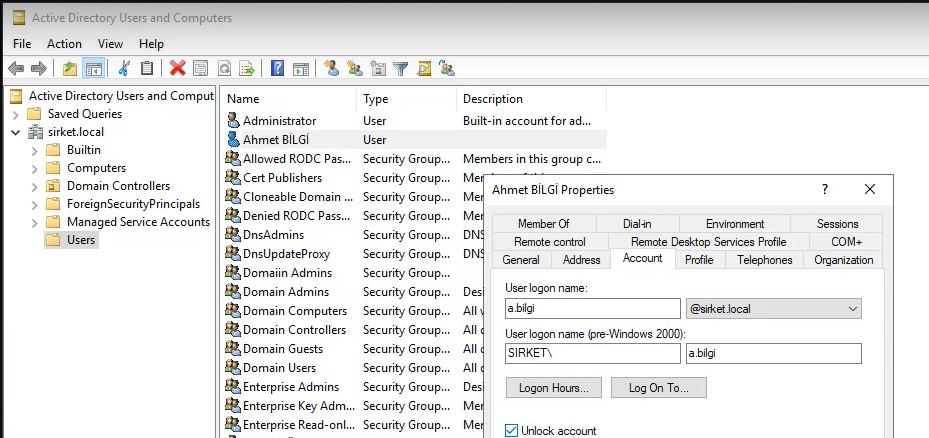
-Güvenlik için min. 10 karakter olması gerekmektedir.

-Verdikleri şifreyi ise belirli günler içerisinde değiştirilmelidir.

-Ayrıca son 24 şifrenin aynı olmaması güvenlik için önemlidir.



-"AccountLockoutPolicy" seçeneğinde ayrıca şifre yanlış girildiğinde Account'u kitlemesini ve kaç dakika sonra aktif kalacağını ayarlayabiliriz.

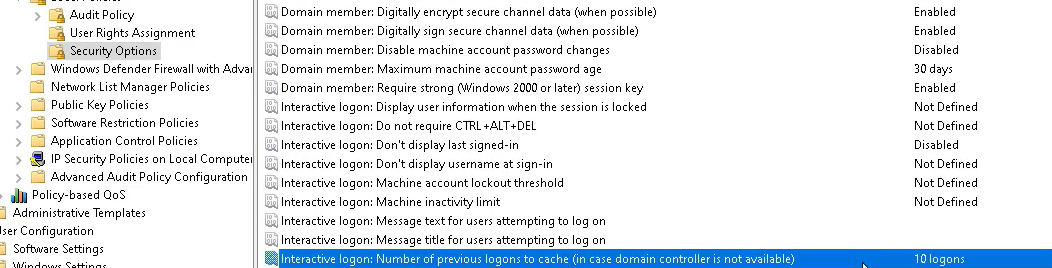


-Kitlenme durumunda ise ActiveDirectory üzerinden listeden kaldırılarak aktif hale getirilebilir.

***Cache Logon’un Kapatılması***

-Cachelogon ->Domain Controller kullanılır olmadığı zaman ortamda 10 kere daha oturum açabilir ve bu şifreyi hafızasında tutar.

-Şirket dışına çıktığında DomainController olmadığından sisteme rahat bir şekilde erişim sağlayabilir.Bunun önüne geçmek için bu sayının azaltılmasında fayda vardır.

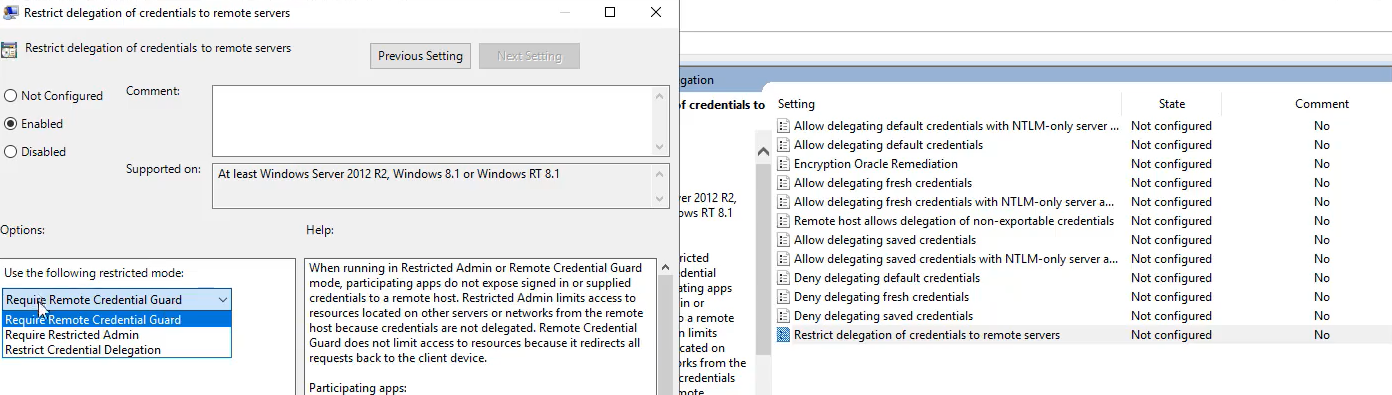


-Bu ayar Local üzerinde "WindowsSet>SecuritySet>LocalPolicies>SecurityOpt." içerisinde bulunur.

-Ayarın 1 yapılması uygundur.

***Restricted Admin Mode’un Etkileştirilmesi***

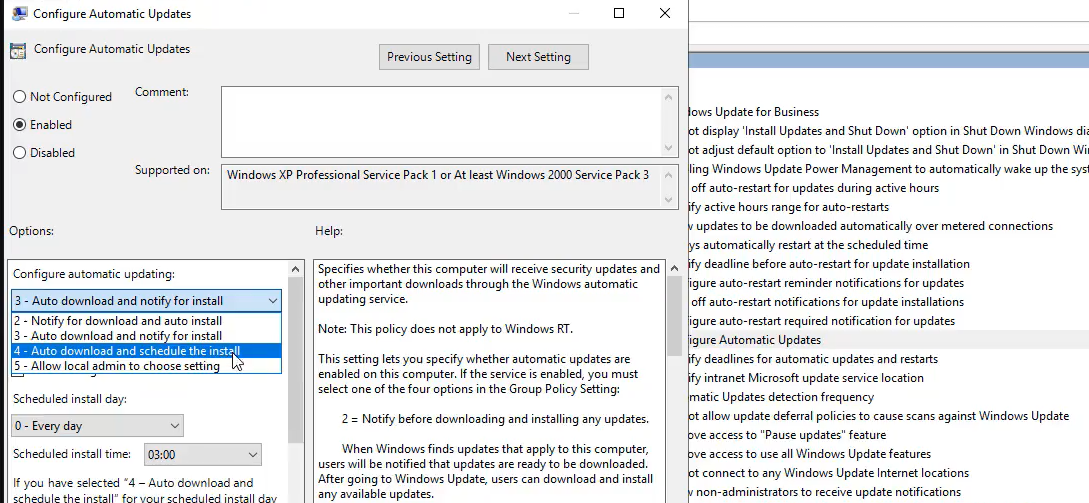
-RDP için Restricted kısıtlı yönetici modunu da aktif etmekte fayda vardır.



-Bu ayara Server üzerinde "Policies>AdministrativeTemplates>System>CredentialsDelegation" içerisinde erişebiliriz.

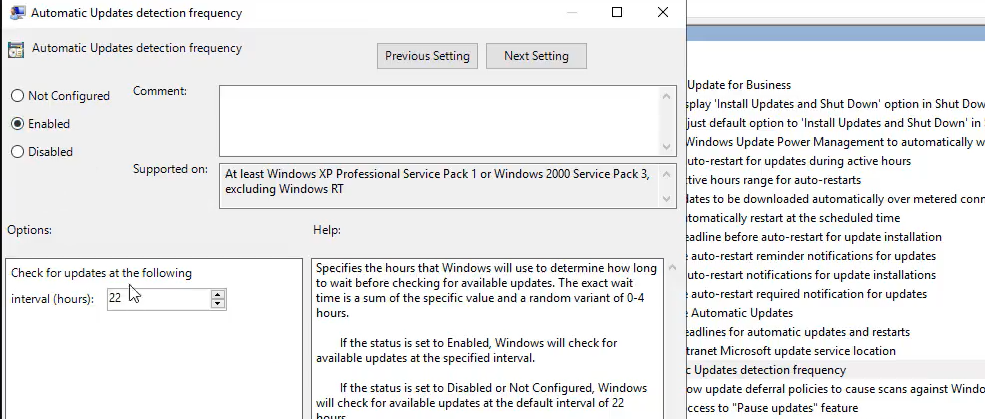
***Güvenlik Güncelleştirmelerine Zorlama***

-Güvenlik Güncellemelerinin öneminin Siber Güvenlikte ne kadar yer kapladığını bilmekteyiz.Bu sebeple güncelleştirmelerini zorunlu hale getirmeliyiz.

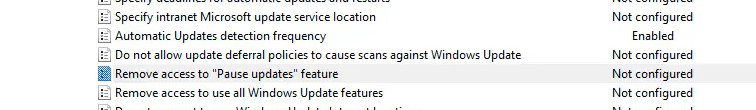


-Server içerisinde Group Policy'a geçiş yapıyorum ve burada System başlığı altında bulunan Windows Update'e geçiş yapıyorum.

-Burada sormadan ve belirli saatlerde zorlayarak güncelleme yapmasını sağlayabiliriz.

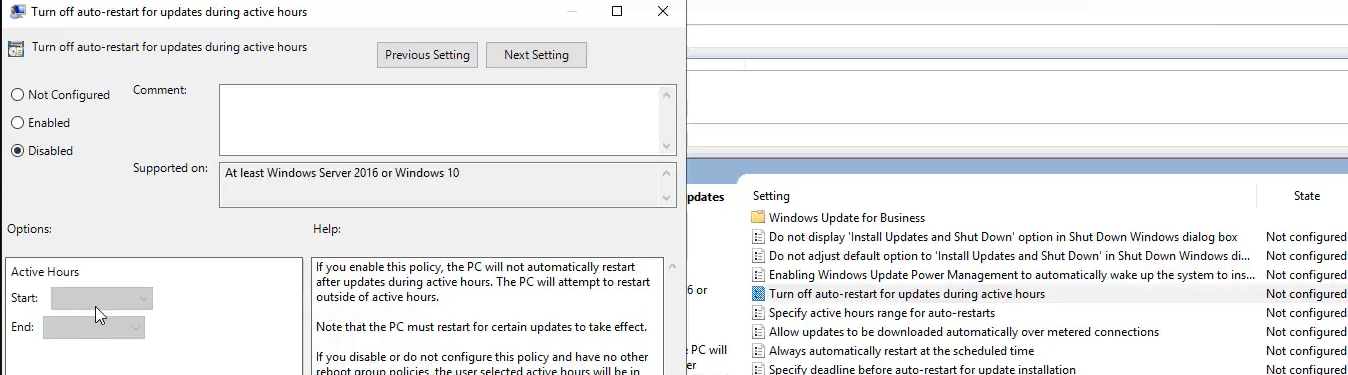


-Güncellemenin haricinde güncelleme tarama zamanını da ayarlayabiliriz.



-"RemoteAccessto" seçeneğini devre dışı bırakıp iptal edemez hale getirebiliriz.

-Ayrıca tüm WindowsUpdate erişimlerini kapatabiliriz.Bu sayede ayarı isteseler de değiştiremezler.

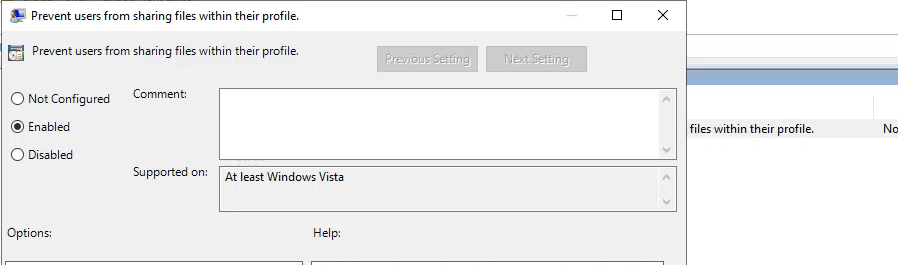


-Güncellemelerin aktif olabilmesi için genellikle sistemin kapatıp açılması gerekmektedir.

-Yeniden başlatma işleminin de belirli saatlerde uygulanması bizim için fayda sağlayacaktır.

***Paylaşım ve NTFS Haklarının Kısıtlanması***

-Güvenlik açısından bir diğer önemli husus ise dosyaların paylaşımıdır.



-Bu açığı Server üzerinde "UserConf>Administrative>WindowsCompenents>NetworkSharing" içerisine geçiş yapıyorum.

-Bu ayarı kapattığım da Server üzerinde daha önce paylaşılmış dosyalara kesinlikle erişim sağlayabilirler.



"OrtakAlan" üzerinde bulunan yetkilere de dikkat edilmektedir.

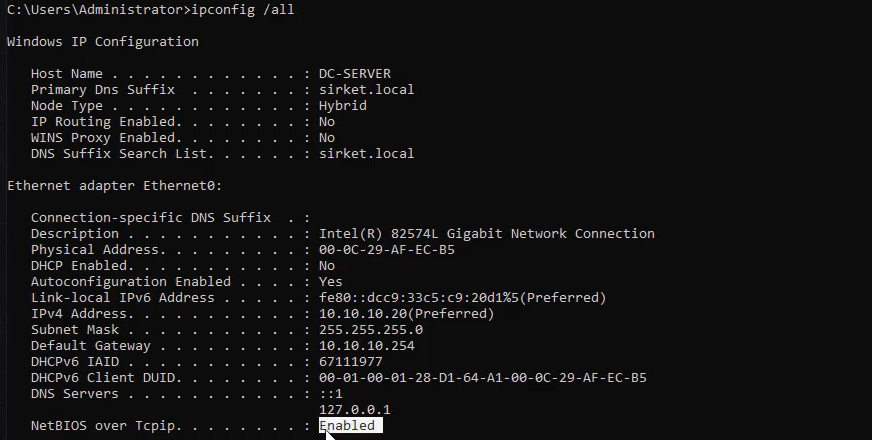
-İçeriğinde ilişkisi bulunmayan kullanıcıların sınıflandırılması kesinlikle önemlidir.(Everyone paylaşımları server içerisinde kullanılmamaktadır.)

-Ayrıca Çalıştır üzerinde yanlış kullanımlarda "Responder" aracı ile yakalayıp zafiyetten yararlanmıştık.Bunun önüne geçmek için erişim sağlayabilecekleri Client'lerin kısayolları Masaüstüne koyulmalıdır.

***LLMNR ve NetBIOS’un kapatılması***

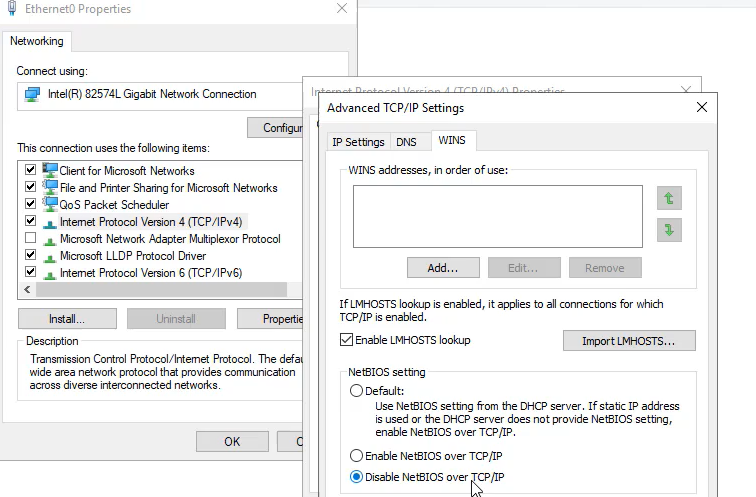
-LLMNR ve NetBIOS üzerinde de yapılması gereken ayarlar vardır.

-LLMNR üzerinden erişim sağladığımızı görüntülemiştik.



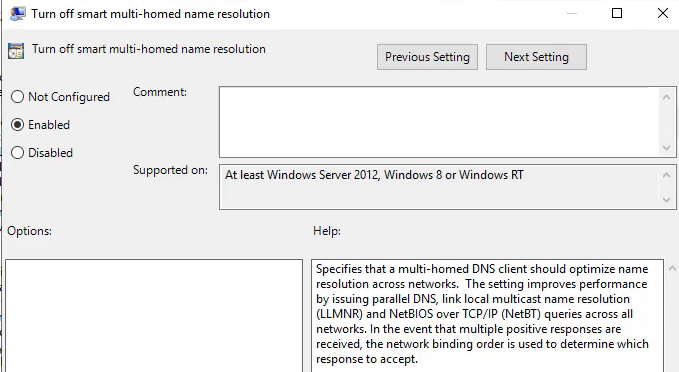
-"ipconfig" komutunu çalıştırdığımız da burada aktif olup olmadığını görüntüleyebiliriz.

-Eğer server üzerinde 2000 öncesi sistem yok ise bu ayarın kapatılması gerekmektedir.



-"IPv4" ayarlarından "Advanced>WINS" içerisine geçiş yaptığımda buradan NetBIOS servisini devre dışı bırakabilirim.

-Ardından Server üzerine geçiş yapıyorum.

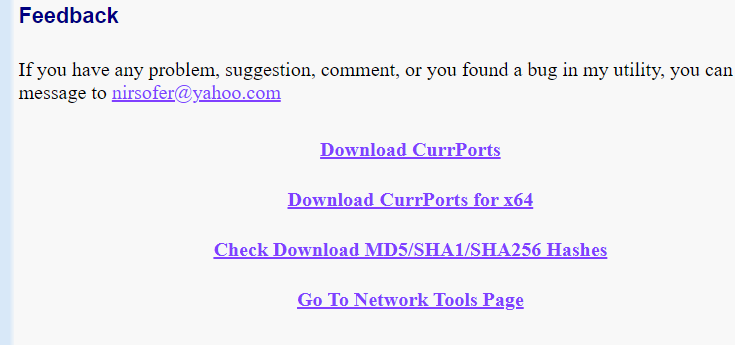


-Burada Default Ayarlara giriyorum ve "Policies>Administrative>Network>DnsClient" içerisine geçiş yapıyorum.

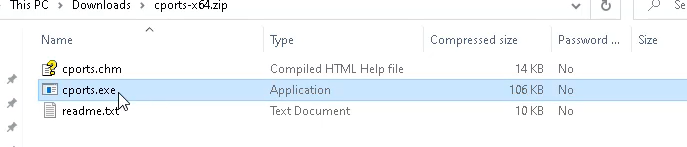
-Görsel üzerinde gösterdiğim servisi devre dışı bırakarak.LLMNR servisine karşı önlem almış oluruz.

***Port Monitoring***

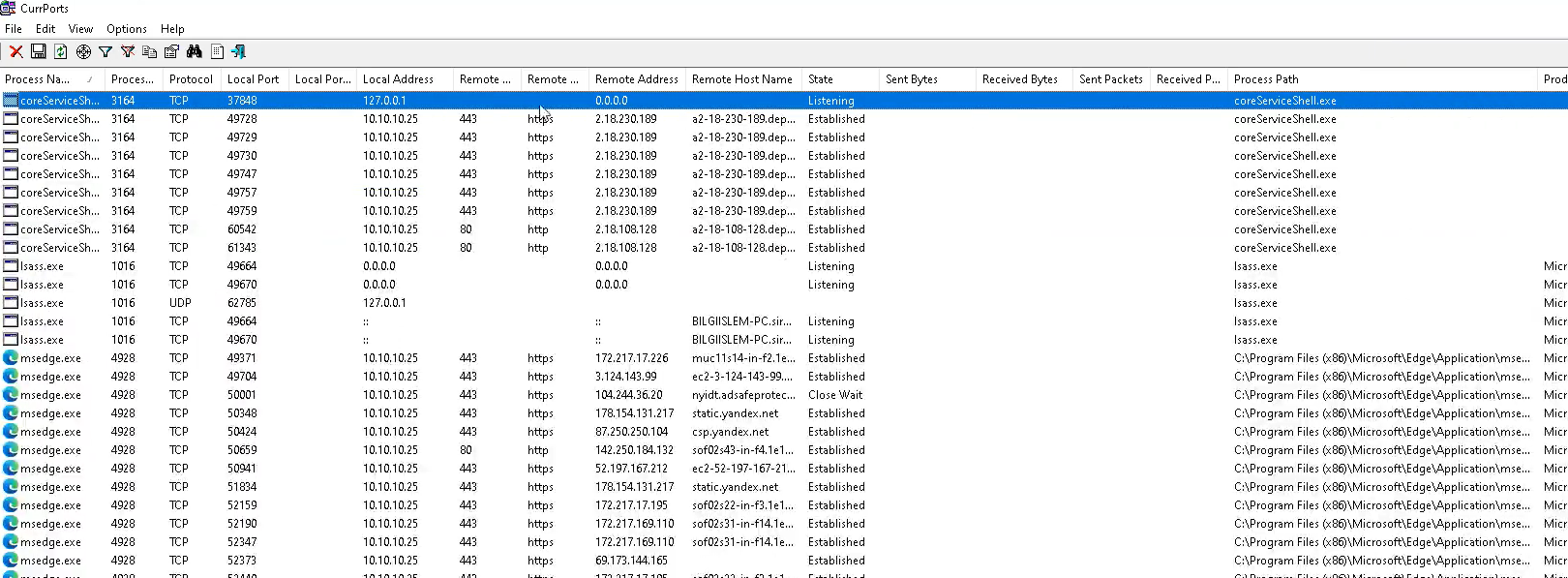
-CurrentPort uygulaması ile portların hangi Cihazlar ile iletişim kurduğunu takip edebilirim.



-"https://www.nirsoft.net/utils/cports.html" bağlantısı üzerinden indirim işlemini sağlayabilirim.



-İçeriğini görüntüledikten sonra aracı başlatıyorum.

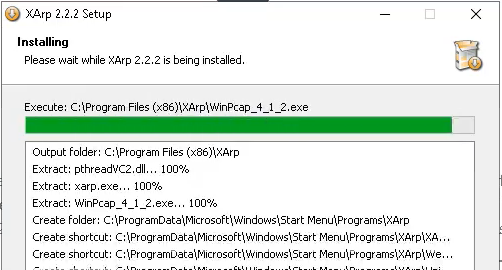


-İletişim kurduğu Ip adresini,Port Adresini,Kullandığı Servisleri burada görüntüleyerek ve kendi eklediğimiz özellikler ile server güvenliğini sağlayabiliriz.

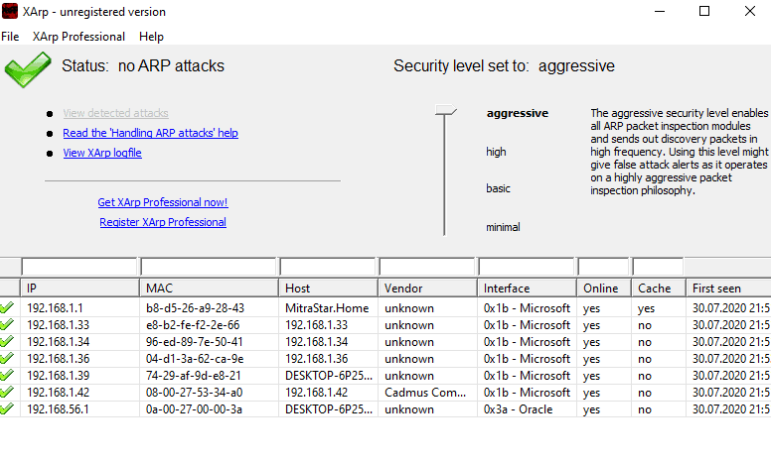
***ARP Poisining Tespiti ve Bildirimi***

-ARP Poisining işlemini durdurmak için Router,Switch gibi cihazlara ihtiyaç vardır.

-Tespiti için Clientler içerisine eklediğimiz "xARP" uygulaması ile ARP saldırısı sırasında bilgi sahibi olabiliriz.



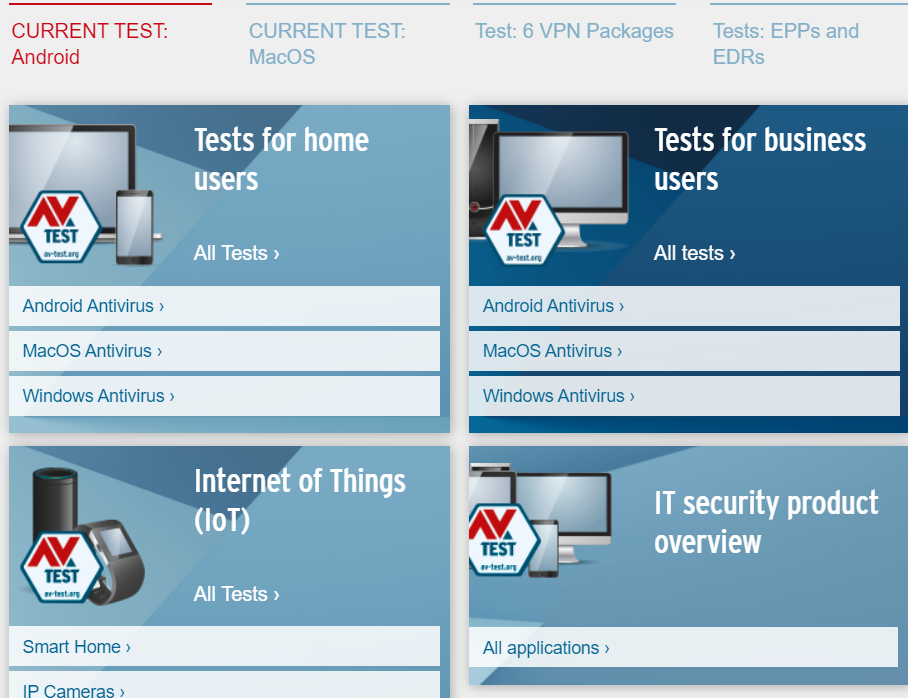
-Bu araca "xarp.net" üzerinden erişim sağlayabiliriz.



-Kurulum sonrasında eğer ki bir saldırı olur ise bu şekilde ekrandan görüntü sağlayabiliriz.

***Antivirüs Testleri ve Seçimi***

-Server üzerinde Antivirüs seçmek ve seçtiğimiz Antivirüs programının güncelliğini koruması çok önemlidir.Bu işlemi bizler için gerçekleştiren tarayıcı üzerinden erişim sağlayabileceğimiz taraflı tarafsız bağlantılar bulunmaktadır.



-Bu bağlantıların başında "https://www.av-test.org/en/" bulunmaktadır.

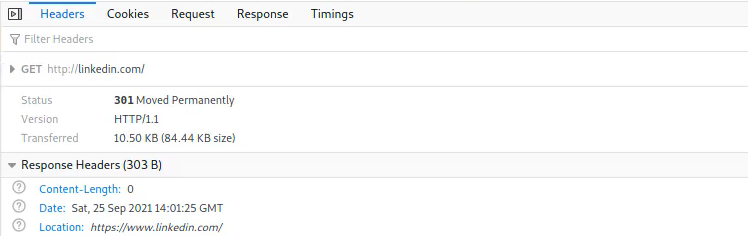
-Sitenin görünümü bu şekildedir.



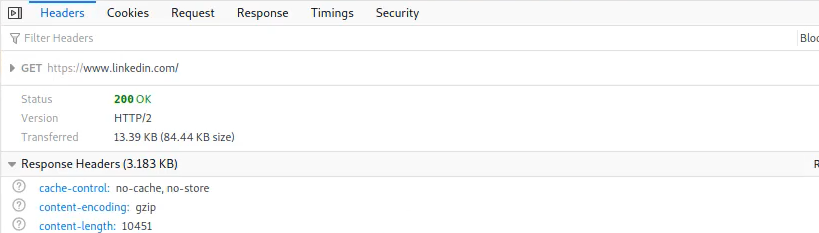
-Örnek olarak ise Ekim ayının en iyi antivirüslerine buradan erişim sağlayabiliyoruz.

***SSL Strip ve HSTS Kavramları***

HSTS: HTTP yerine HTTPS bağlantısı ile hizmet verilmesini sağlar.Tarama yerinde HTTP belirtilmediğinde HTTPS olarak dönmesini sağlar.Bu servis sunucuda çalışır.

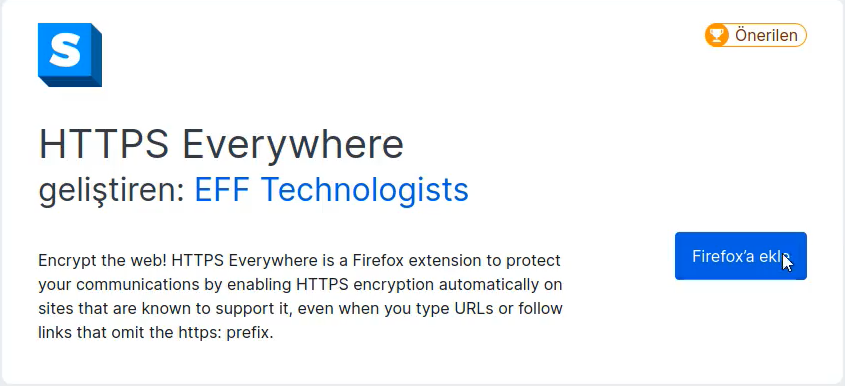


-"linkedin.com" bağlantısı üzerine arama gerçekleştiriyorum.Burada ilk gönderdiğim paket HTTP olarak gidiyor fakat 301 hatası döndürüyor.



-301 hata kodu sonrasında HTTPS üzerinden bağlantı sağladım.Kaynak kodunda HSTS kuralının kaç saniye çalışacağını görüntülüyorum.

Bu zafiyetten yararlanılması halinde SSL Strip işlemi gerçekleştirilir.



-HTTP sayfalarına bağlanmasını engellemek için Server üzerinde bulunan cihazların Tarayıcılarına "HTTPS Everywhere" eklentisini ekleyebilirim.Bu eklenti sayesinde HTTPS olarak bağlantı yapmaya zorlayabilirim.