Gazi Üniversitesi
Fen Bilimleri Dergisi
PART C: TASARIM VE TEKNOLOJİ

Gazi University
Journal of Science
PART C: DESIGN AND TECHNOLOGY

GU J Sci, Part C, 12(3): 475-487 (2024)

Windows Aktif Dizin Etki Alanı Servisi ve Kurumsal Ağ Güvenliği: PowerShell Erişiminin Analizi ve Önlemler

Zeynep ŞENTÜRK[1*] Erdal IRMAK[2]

[1]*Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Bilgi Güvenliği Mühendisliği Ana Bilim Dalı, Ankara, Türkiye*

[2]*Gazi Üniversitesi, Teknoloji Fakültesi, Elektrik Elektronik Mühendisliği Bölümü, Ankara, Türkiye*

Makale Bilgisi

Araştırma makalesi
Başvuru: 06/03/2024
Düzeltme: 13/05/2024
Kabul: 30/05/2024

Anahtar Kelimeler

Windows aktif dizin etki Alanı servisi
PowerShell
Etki alanı sızma testi

Article Info

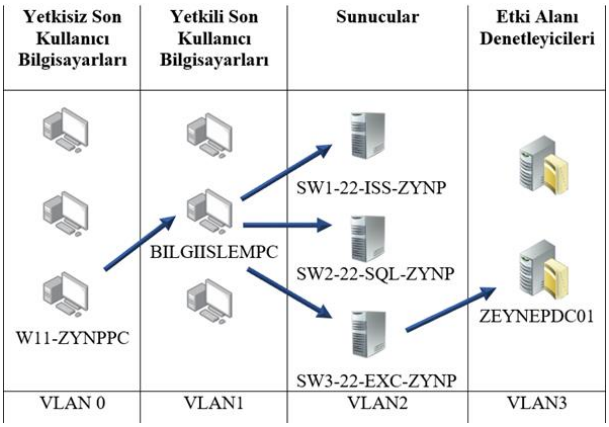
Research article
Received: 06/03/2024
Revision: 13/05/2024
Accepted: 30/05/2024

Keywords

Windows active directory Domain service
PowerShell
Domain penetration testing

Grafik Özet (Graphical/Tabular Abstract)

Bu çalışmada, temsili kurumsal ağ üzerinde PowerShell kullanılarak bir etki alanı sızma testi gerçekleştirilmiştir. Sızma testi senaryosunda, yetkisiz son kullanıcı bilgisayarında oturum açan yetkisiz saldırgan profilinin, etki alanı denetleyicisine erişim adımları işlenmiştir. / In this study, a domain penetration test was carried out using PowerShell on a representative enterprise network. In the penetration test scenario, the steps of the unauthorized attacker profile logging in to the unauthorized end user computer to access the domain controller are covered.



Şekil A: *Etki alanı sızma testi senaryosu / Domain penetration test scenario*

Önemli noktalar (Highlights)

- *PowerShell erişiminin, kurumlar için oluşturduğu risk ve tehlikenin incelenmesi. / Examining the risk and danger that PowerShell access poses for institutions*
- *Kurumsal ağda bulunan potansiyel zafiyetlerin incelenmesi. / Examining potential vulnerabilities in the enterprise network.*
- *Windows Aktif Dizin Etki Alanı Servisi güvenliği için alınabilecek önlemlerin sunulması. / Presenting the precautions that can be taken for Windows Active Directory Domain Service security*

Amaç (Aim): *Bu çalışmanın amacı, kurumsal ağlarda PowerShell erişiminin oluşturduğu güvenlik risklerini incelemek ve bu risklere karşı önlemler sunmaktır. / The purpose of this study is to examine the security risks posed by PowerShell access in enterprise networks and to offer precautions against these risks.*

Özgünlük (Originality): *Literatür incelendiğinde, kurumsal ağ güvenliği konusu çalışmada olduğu gibi PowerShell erişimi bakış açısıyla değerlendirilmemiştir. / When the literature is examined, corporate network security has not been evaluated from the perspective of PowerShell access as in the study.*

Bulgular (Results): *Kurumlarda PowerShell erişimi, etki alanı güvenliği açısından risk oluşturmaktadır. / PowerShell access in organizations poses a risk to domain security.*

Sonuç (Conclusion): *Kurumlarda etki alanı güvenliğinin artırılması için PowerShell erişimi, kullanıcılara kapatılmalıdır. / To increase domain security in organizations, PowerShell access should be closed to users.*

*Corresponding author, e-mail: zeynep.senturk1@gazi.edu.tr
DOI: 10.29109/gujsc.1447924

GU J Sci, Part C, 12(3): 475-487 (2024)

Gazi Üniversitesi
Fen Bilimleri Dergisi
PART C: TASARIM VE TEKNOLOJİ

Gazi University
Journal of Science
PART C: DESIGN AND TECHNOLOGY

http://dergipark.gov.tr/gujsc

Windows Aktif Dizin Etki Alanı Servisi ve Kurumsal Ağ Güvenliği: PowerShell Erişiminin Analizi ve Önlemler

Zeynep ŞENTÜRK[1*] Erdal IRMAK[2]

[1] *Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Bilgi Güvenliği Mühendisliği Ana Bilim Dalı, Ankara, Türkiye*

[2] *Gazi Üniversitesi, Teknoloji Fakültesi, Elektrik Elektronik Mühendisliği Bölümü, Ankara, Türkiye*

Makale Bilgisi

Araştırma makalesi
Başvuru: 06/03/2024
Düzeltme: 13/05/2024
Kabul: 30/05/2024

Anahtar Kelimeler

Windows aktif dizin etki Alanı servisi
PowerShell
Etki alanı sızma testi

Öz

Bu çalışma, Microsoft tarafından geliştirilen ve organizasyonlar için kritik bir bilgi teknolojileri bileşeni olan Windows Aktif Dizin Etki Alanı Servisi'ni ele almaktadır. Bu servis, sunduğu yüksek işlevsellikle dünya genelinde yaygın bir şekilde kullanılmaktadır, ancak aynı zamanda kurumları siber saldırılara karşı savunmasız kılan bir hedef haline gelmiştir. Bu nedenle çalışmada öncelikle Windows PowerShell kabuk katman ortamının kurumsal ağlar için potansiyel tehlikeleri ortaya konulmuştur. Örnek bir kurumsal ağ ortamında Windows Aktif Dizin Etki Alanı Servisi kullanılarak, yetkisiz bir kullanıcı oturumu açan kötü niyetli personelin ağ üzerinde gerçekleştirebileceği saldırılar uygulamalı olarak incelenmiştir. Sonuçlar, kurum içinde personelin kabuk katmana erişebilmesinin büyük güvenlik riskleri oluşturduğunu göstermektedir. Kurumların bu tür saldırılardan korunması amacıyla kabuk katman ortamının güvenliğini artıracak ve potansiyel saldırıları engellemek için etkili bir strateji oluşturmayı amaçlayan önlemler tartışılmıştır. Çalışmanın, kurumsal ağların güvenliğine önemli katkılar sağlayacağı değerlendirilmektedir.

Windows Active Directory Domain Services and Enterprise Network Security: Analysis and Measures for PowerShell Access

Article Info

Research article
Received: 06/03/2024
Revision: 13/05/2024
Accepted: 30/05/2024

Keywords

Windows active directory
Domain service
PowerShell
Domain penetration testing

Abstract

This study discusses the Windows Active Directory Domain Service, developed by Microsoft, and a critical information technology component for organizations. This service is widely used around the world because of the high functionality it offers, but it has also become a target that makes organizations vulnerable to cyber-attacks. For this reason, in the study, first of all, the potential dangers of the Windows PowerShell shell layer environment for corporate networks are revealed. Using the Windows Active Directory Domain Service in a sample corporate network environment, the attacks that can be carried out on the network by malicious personnel who log in to an unauthorized user have been practically examined. The results show that internal personnel access to the shell layer poses major security risks. To protect institutions from such attacks, measures that will increase the security of the shell layer environment and aim to create an effective strategy to prevent potential attacks are discussed. It is evaluated that the study will make significant contributions to the security of corporate networks.

1. GİRİŞ (INTRODUCTION)

Microsoft firmasının sahibi olduğu Windows işletim sistemi, küresel ölçekte en yaygın kullanılan bilgisayar işletim sistemi olarak baskın konuma sahiptir [1]. Microsoft, bir dizin hizmeti olarak Aktif Dizin Etki Alanı Servisi'ni Windows 2000 sunucu işletim sistemiyle piyasaya sürmüştür [2]. Entegrasyon kolaylığı ve yönetimi kolaylaştırması nedeniyle aktif dizin servisi piyasaya sürüldüğünden beri işletmeler için önemli bir altyapı bileşeni haline gelmiştir. Etki alanı yapısı bu dizin hizmetinin bir parçasıdır. Her etki alanının, Domain Controller olarak ifade edilen en az bir etki alanı denetleyicisi vardır ve etki alanı denetleyicisi bu etki alanının en yetkili ve kritik sunucusudur. Aktif dizin servisi; merkezi yönetim imkânı, kullanıcıların yetkilendirme işlemlerinin gruplandırılarak yapılabilmesi, kimlik doğrulaması yapılabilmesi, replikasyon özelliği ile veri tabanının

*Corresponding author, e-mail: zeynep.senturk1@gazi.edu.tr
DOI: 10.29109/gujsc.1447924

aktarımının yapılabilmesi gibi özellikleri sebebiyle saldırganlar için önemli bir hedef haline gelmektedir. Saldırılar sonucunda kurumlar, veri kayıplarının yanı sıra finansal olarak da önemli kayıplara uğramaktadır [3].

Kurum ve kuruluşlara yapılan siber saldırlar her zaman dışarıdan gelmemektedir. Kurum personeli, siber güvenlik açısından birer iç tehdit olarak değerlendirilebilir. Kötü niyetli personel veya ihmalkâr davranışlar güvenlik açısından olumsuz sonuçlar doğurabilir. Etki alanına üye bir bilgisayarı ele geçirmiş olan bir saldırgan ile kurum bilgisayarında oturum açma yetkisine sahip kötü niyetli bir kurum personeli aynı saldırı vektörlerini koşturabilir. Ponemon Enstitüsü tarafından hazırlanan "2022 İçeriden Gelen Tehditlerin Maliyeti" raporuna göre iç tehdit olayları son iki yılda %50 artmıştır. Raporda saldırıların yarısından fazlasının ihmalden, dörtte birinin kötü niyetli kişilerden, geri kalan kısmının ise kimlik hırsızlığından kaynaklandığı belirtilmiştir [4]. Bu oldukça ciddi bir artış oranına işaret etmektedir. İç tehditlerin yeterince ciddiye alınmaması, bu artışın temel sebeplerinden biridir. İçeriden gelen tehditler şirketler için ciddi veri ihlallerine sebep olmaktadır. Fortinet, bilgi teknolojileri uzmanlarıyla yaptığı ankette; dolandırıcılık (%55), parasal kazançlar (%49) ve fikri mülkiyet hırsızlığının (%44) içeriden tehdit saldırısının gerçekleşmesinin en büyük üç nedeni olduğunu ortaya koymuştur [5].

2022'de dünyanın en büyük şirketlerinden biri olan Microsoft, içeriden bir saldırıya uğramıştır. Birden fazla çalışanın, GitHub'daki şirketin altyapısına ait hassas oturum açma giriş bilgilerini sızdırdığı tespit edilmiştir. Bu durum tüm şirketi tehlikeye atarak saldırganların Azure sunucularına ve Microsoft'un diğer dâhili sistemlerine erişmesine imkân sağlamıştır [6]. Yine dünya çapında büyük şirketlerden biri olan Tesla şirketinin bir çalışanı, büyük miktarda son derece hassas olan verileri çalarak bunları bilinmeyen üçüncü taraflara göndermek için şirketin ağına olan güvenilir erişimini kullanmıştır [7].

Kurumların siber saldırılardan korunmak için aldığı önemli tedbirlerden bir tanesi sızma testi uygulamalarıdır. Sızma testleri, sistemleri daha güvenli hale getirmek amacıyla zafiyetleri bulmak ve bu zafiyetlerin nasıl kapatılacağı konusunda yol göstermek için yapılan yasal siber saldırı çalışmalarıdır [8]. Kurumlar sızma testleri için; dış ağ, iç ağ, web uygulamaları, kablosuz ağ, sosyal mühendislik, Dağıtık Hizmet Engelleme (DDoS), etki alanı ve fiziksel güvenlik gibi birçok farklı alan içerisinden kendi test kapsamlarını belirlerler. Bu çalışma kapsamında ise etki alanı sızma testine odaklanılmıştır.

Etki alanı saldırıları keşif aşaması ile başlar ve aktif dizin nesneleriyle ilgili bilgiler toplanır. Keşif aşamasında; mevcut etki alanı yapısı, kullanıcı hesapları, makineler, ayrıcalıklı gruplar, Erişim Kontrol Listesi (ACL) girişleri, grup ilkeleri, servisler hakkında bilgi toplanır [9]. Toplanan bilgiler aktif dizin üyesi diğer nesneler üzerinde kullanılmaya çalışılır. Windows etki alanı saldırılarının nihai hedefi, Windows etki alanı yönetici ayrıcalıkları kazanmak ve böylece tüm etki alanı bileşenleri üzerinde kontrol elde etmektir [10]. Keşif aşamasından sonra, daha fazla işlem kabiliyeti elde etmek için yetki yükseltme saldırıları gerçekleştirilmektedir. Aktif dizin ortamında yetki yükseltme aşamasında; genel olarak PassTheHass saldırısı [11], Kerberosting saldırısı [12] ve hatalı nesne yapılandırmalardan yararlanılmaktadır. Saldırılarda; mantıksal, yazılımsal ve yapılandırma kaynaklı hatalar üzerine yoğunlaşılarak etki alanı denetleyicisinin ele geçirilmesi hedeflenmektedir. Hedef bu olsa dahi etki alanı denetleyicisinin ele geçirilemediği fakat etki alanına üye birçok kritik bilgisayarın ele geçirildiği durumlar da mümkündür. Hedefledikleri sistemlere erişebilen saldırganlar bu ortamda mümkün olduğunca uzun kalmak için kalıcılık sağlama yöntemlerine başvururlar.

Sızma testlerinde kullanılmak üzere çeşitli araçlar mevcuttur. Bu çalışmada, desteklenen tüm Windows sürümlerine varsayılan olarak gelen PowerShell aracı ile sızma testi gerçekleştirilmiştir. PowerShell; Microsoft.NET çerçevesinde oluşturulmuş güçlü bir komut dosyası dili, bir komut satırı kabuğu ve görev odaklı komut dosyası oluşturma platformudur [13]. Çok çeşitli kitaplıklar, kullanışlı yerel PowerShell komutları ve çok yönlülüğü nedeniyle bilgi teknolojileri operatörleri için kolaylıklar sağlamaktadır. PowerShell ile Windows Dinamik Bağlantı Kitaplıkları (DLL) fonksiyonları çağrılabilir. PowerShell, Windows sistemlerini yönetme ve görevleri otomatikleştirme konusunda işlevsellik ve esneklik sağladığından özellikle sistem yöneticileri tarafından sıklıkla kullanılmaktadır. PowerShell'in sağlamış olduğu esnekliklerin kötü niyetli kişiler tarafından kullanılması, sistem için büyük güvenlik açıklıkları oluşturabilir. Saldırganlar, ayak izlerini azaltabilirler ve savunma mekanizmalarından kaçabilirler. 2016 yılında açık kaynaklı bir proje olarak sunulan Powershell 6.0 (Powershell Core), bazı büyük Linux dağıtımlarında ve MacOS dahil olmak üzere birçok farklı platformda kullanılabilmektedir [14].

Sızma testleri ile ilgili yapılan literatür taramasında; çalışma [15]'de sızma testi araçları incelenerek Kali Linux'te bulunan 6 farklı başlığı kapsayan 18 farklı araç incelenmiştir. Araçların kabiliyetleri gösterilerek ücretsiz olan bu araçların kötü niyetli kişiler tarafından kullanılırsa ne kadar zararlı olabilecekleri vurgulanmıştır. Çalışma [16]'da, siber korsanların ve sızma testi ekiplerinin sıklıkla kullandığı Metasploit Framework aracının kabiliyetleri anlatılmıştır. Metasploit Framework'e ait bir araç olan "msfvenom" ile ilgili kısa bir uygulama çalışması yapılarak sonuçları paylaşılmıştır.

Sızma testlerinde kullanılan bir diğer araç olan ağ haritalama (Nmap) aracının anlatıldığı çalışma [17]'de, bu aracın kullanım alanlarından bahsedilmiştir. Nmap parametrelerinden bazılarının işlevi anlatılarak, kullanımı ve sonuçları paylaşılmıştır. Çalışma [18]'de, Nmap aracına karşı bir algılama yaklaşımı olarak, kapsamlı Nmap tespit kuralları önerilmiştir. Saldırı Tespit Sistemleri (IDS)'nin Nmap taramalarını tespit etme konusunda yetersiz olduğuna dikkat çekilmiştir. Bir test ortamı kurularak önerilen kurallar çerçevesinde bir deney yapılmıştır. Yüksek doğruluk oranına sahip sonuçlar elde edilmiştir.

Çalışma [19]'da yazarlar, saldırganların kurumsal yapıdaki saldırı yüzeyini genişletmek için kullandıkları yanal hareket tekniğini ele almıştır. Bu saldırı tekniğinin tespit edilmesindeki sorunlara değinilmiş ve yanal hareket saldırılarına karşı alınabilecek önlemlere yer verilmiştir. Sızma testleriyle ilgili yapılan çalışma [20]'de, sızma testi metodolojileri, stratejileri ve sızma testi araçları anlatılmıştır. Sızma testlerinde kullanılan araçlar işlevleri ile birlikte tablo halinde sunulmuştur. Tanıtılan sızma testi araçlarından ücretsiz olan araçların kabiliyeti gösterilerek bu araçların kötü niyetli kişiler tarafından kullanılması ihtimaline değinilerek sızma testlerinin önemi vurgulanmıştır. İncelenen çalışmalar sonucunda, sızma testi çalışmalarının büyük oranda Kali Linux işletim sistemi kullanılarak gerçekleştirildiği görülmüştür. Bunun sebebi, Kali Linux işletim sisteminde mevcut olan saldırı araçlarıdır.

Daha önce PowerShell ile ilgili yapılan çalışmalardan [21]'de, sızma testi sırasında kullanabilecek Empire ve Nishang araçlarının PowerShell'de kullanımına yer verilmiştir. Test sırasında kullanılabilecek birkaç komuttan bahsedilmiş olsa da çalışmadaki açıklama ve uygulamalar oldukça kısıtlıdır. Konuyla ilgili bir diğer kaynak olan [22]'de, aktif dizin saldırılarına değinilmiş ve PowerShell'in bazı komut ve araçlarının bu saldırılarda kullanılabileceğinden bahsedilmiştir. Fakat çalışmada, PowerShell ile yapılabilecek bir sızma testi mevcut değildir. Bu iki çalışma haricinde kaynaklar taranmış olsa da literatürde konuyla ilgili Türkçe kaynak eksikliği dikkat çekmektedir.

Yukarıda kısaca özetlenen motivasyonla bu çalışmada, işlevselliği ve yaygın kullanımı nedeniyle siber saldırılara karşı popüler bir hedef olan Windows Aktif Dizin Etki Alanı Servisi siber güvenlik boyutuyla incelenerek Windows PowerShell kabuk katman ortamının potansiyel tehlikeleri üzerinde durulmuştur. Bu amaçlarla çalışmada bir kurum bilgisayarlarında kabuk katmanı -PowerShell- erişimi olan yetkisiz bir kullanıcının, kurum için oluşturabileceği güvenlik risklerini görebilmek amacıyla bir uygulama sunulmuştur. Uygulama çalışması için oluşturulan temsili kurumsal ağ üzerinde, yetkisiz bir kullanıcı hesabı aracılığıyla bir sızma testi gerçekleştirilmiştir. Bu sızma testi senaryosunun özgünlüğü, çalışmanın yenilikçi yönünü oluşturmaktadır. Ayrıca, kabuk katmanına erişimi olan kötü niyetli bir kullanıcının ağda gerçekleştirebileceği saldırılar paylaşılmıştır. Çalışmanın özellikle Windows PowerShell aracılığıyla yetkisiz erişimleri ve içeriden yapılabilecek saldırıları detaylı bir şekilde sunmasıyla literatüre katkı sağlayacağı ve güvenlik zafiyetlerinin istismarını örneklemek için gerçek saldırı vektörleri ve senaryoları üzerinden uygulamaları içermesiyle kritik bir öneme sahip olacağı değerlendirilmektedir. Ayrıca, kabuk katman ortamının güvenliğini artırmak ve potansiyel saldırıları engellemek için önerilen stratejiler, kurumların güvenlik politikalarını güçlendirmelerine yardımcı olacaktır.

2. POWERSHELL İLE ETKİ ALANI SIZMA TESTİ (DOMAIN PENETRATION TESTING WITH POWERSHELL)

Bu bölümde, çalışma için sanal ortamda oluşturulan temsili kurumsal bir ağ üzerinde etki alanı sızma testi gerçekleştirilmiştir. Bu sızma testinin amacı; Windows etki alanı servisi kullanılan organizasyonlarda, yetkisiz bir kullanıcının, ek bir işletim sistemi kurmaksızın, Windows'ta yerleşik olarak bulunan PowerShell'i kullanarak gerçekleştirebileceği saldırıları incelemektir.

Sızma testlerinde kullanılan farklı metodolojiler mevcuttur. Bunlardan yaygın olanları; Açık Kaynak Güvenlik Testi Metodoloji Kılavuzu (OSSTMM), Açık Web Uygulama Güvenliği Projesi (OWASP), Bilgi Sistemleri Güvenliği Değerlendirme

Çerçevesi (ISSAF) ve Sızma Testi Uygulama Standardı (PTES) ve Ulusal Standartlar ve Teknoloji Enstitüsü (NIST)'e ait metodolojidir [23]. Bu metodolojiler incelenerek bu çalışmada gerçekleştirilecek olan etki alanı sızma testi için en uygun metodoloji çıkarılarak Şekil 1'de gösterilmiştir.

Kullanıcı, etki alanına üye "W11-ZYNPPC.zynp.com" bilgisayarını kullanmaktadır. Senaryoda, zsenturk@zynp.com" kullanıcısının etki alanı zafiyetlerini PowerShell ile sömürerek en yetkisiz profilden, en yetkili profil olan "Domain Admins" grubuna üye olma süreci işlenmiştir (Şekil 2).

Bu süreçteki zafiyetlerin sömürülmesine dair ekran alıntıları paylaşılarak kullanılan etki alanı atak vektörleri paylaşılmıştır. Bu ortamda gerçekleştirilebilecek olan saldırıda hedef; aktif dizin servisine üye olan mümkün olduğunca çok bilgisayara erişim sağlamak, erişim sağlanan bilgisayarlardan bilgi toplamak ve nihai olarak etki alanı denetleyicisini ele geçirmektir.

Temsili kurumsal ağ ortamı için 6 adet en güncel Windows işletim sistemine sahip sanal bilgisayar kurulmuştur. Deney ortamı için kullanılan cihazın özellikleri Tablo 1'de sunulmuştur. Sanallaştırma platformu olarak, VMware Workstation 17 Pro [24] kullanılmıştır. "zynp.com" adında bir etki alanı oluşturulmuştur. Bu etki alanında yer alan bilgisayarlar Tablo 2'de listelenmiştir. "zynp.com" etki alanına yapılacak olan sızma testi çalışmasında, etki alanında ve etki alanı üyesi bilgisayarda oturum açma yetkisi dışında herhangi bir yetkisi veya ayrıcalığı bulunmayan "zsenturk@zynp.com" kullanıcı hesabı kullanılmıştır.

Şekil 1. Sızma testi metodolojisi (Penetration testing methodology)

Tablo 1. Temsili kurumsal ağ kurmak için kullanılan cihazın özellikleri (Features of the device used to establish a representative enterprise network)

Cihaz	Özellikleri
CPU	Intel i9 13900K
RAM	64 Gbyte 5200 Mhz
İşletim Sistemi	Windows 11- 64 bit
Grafik İşlemci	Nvdia RTX 4080

Tablo 2. Deney ortamında bulunan bilgisayarlar hakkında bilgiler (Information about the computers in the experimental environment)

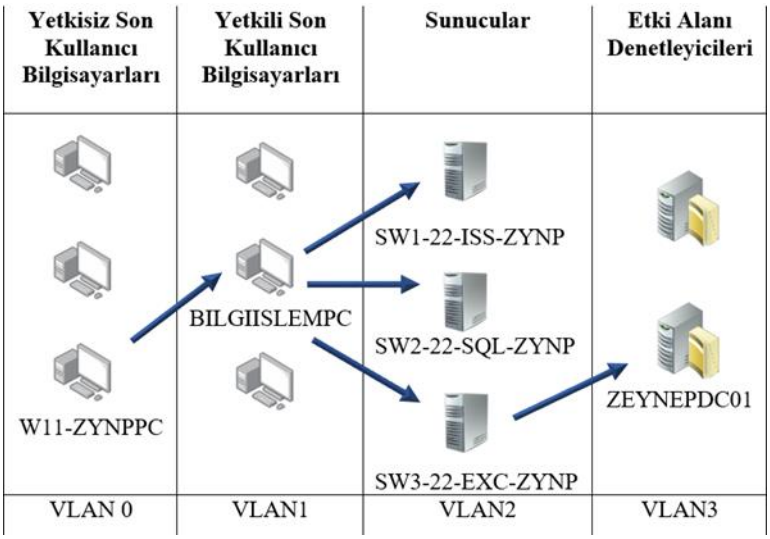
İşletim Sistemi	Bilgisayar Adı	Bilgisayar IP	Bilgisayar Rolü
Windows 11	W11-ZYNPPC.zynp.com	192.168.0.109/24	Standart Yetkili Bilgisayar
Windows 11	BILGIISLEMPC.zynp.com	192.168.1.108/24	Sistem Yöneticisi Bilgisayarı
Windows Server 2022	SW1-22-ISS-ZYNP.zynp.com	192.168.2.106/24	IIS Sunucu Bilgisayarı

Tablo 2'nin devamı

Windows Server 2022	SW2-22-SQL-ZYNP.zynp.com	192.168.2.105/24	SQL Sunucu Bilgisayarı
Windows Server 2022	SW3-22-EXC-ZYNP.zynp.com	192.168.2.110/24	Exchange Sunucu Bilgisayarı
Windows Server 2022	ZEYNEPDC01.zynp.com	192.168.3.100/24	Etki Alanı Denetleyicisi

Bu çalışmada, erişim kontrolü ile daha güvenli bir ağ yapısı oluşturmak amacıyla sanal yerel alan ağı (VLAN) yapılandırmasından yararlanılmıştır. Bilindiği üzere VLAN yapılandırması, farklı katmanları veya işlevleri bölümlere ayırarak ve izole ederek ağ trafiğini optimize etmek için kullanılan bir yöntemdir ve trafiği mantıksal olarak ayırarak yönetim kolaylığı ve güvenlik sunar. Aynı zamanda esneklik ve ölçeklenebilirlik sağlayarak fiziksel altyapıyı değiştirmeden yeni VLAN'ların oluşturulmasına olanak tanır. Çalışmada, VMware Workstation'da yer alan "Sanal Ağ Düzenleyicisi" seçeneğinden "ağ ekle" seçeneği ile VLAN'lar için sanal anahtar oluşturularak her VLAN'a bir numara verilmiştir. Sanal makineler ilgili VLAN'lara bağlanılmıştır. IP adresleri atanarak "custom" mod üzerinden konfigürasyonlar tamamlanmıştır. Network trafik akışını yönlendirmek için Erişim Kontrol Listeleri (ACL) kullanılmıştır. Bu listeler ağ trafiğini filtrelemek için VLAN'larla birlikte kullanılabilir ve ağ yöneticilerinin belirli kullanıcılara veya cihazlara erişimi kontrol etmesine olanak tanır. Ağ yöneticileri, bir VLAN'a erişim izni verilen belirli IP adreslerinden gelen trafiğe izin vererek ağ güvenliğini artırabilir ve yetkisiz erişimi önleyebilir. Erişim kontrol listelerinin bu şekilde kullanımı ağ trafiğinin güvenliğini sağlamada önemli bir adımdır ve VLAN yapılandırmasında yaygın olarak kullanılır. Bu nedenle bu çalışmada da Şekil 2'de gösterildiği gibi 4 farklı VLAN oluşturulmuştur. Bunlar, erişim imkânları en kısıtlı olandan en geniş olanına doğru sırasıyla; VLAN0, VLAN1, VLAN2 ve VLAN3 olacak şekilde ayarlanmıştır

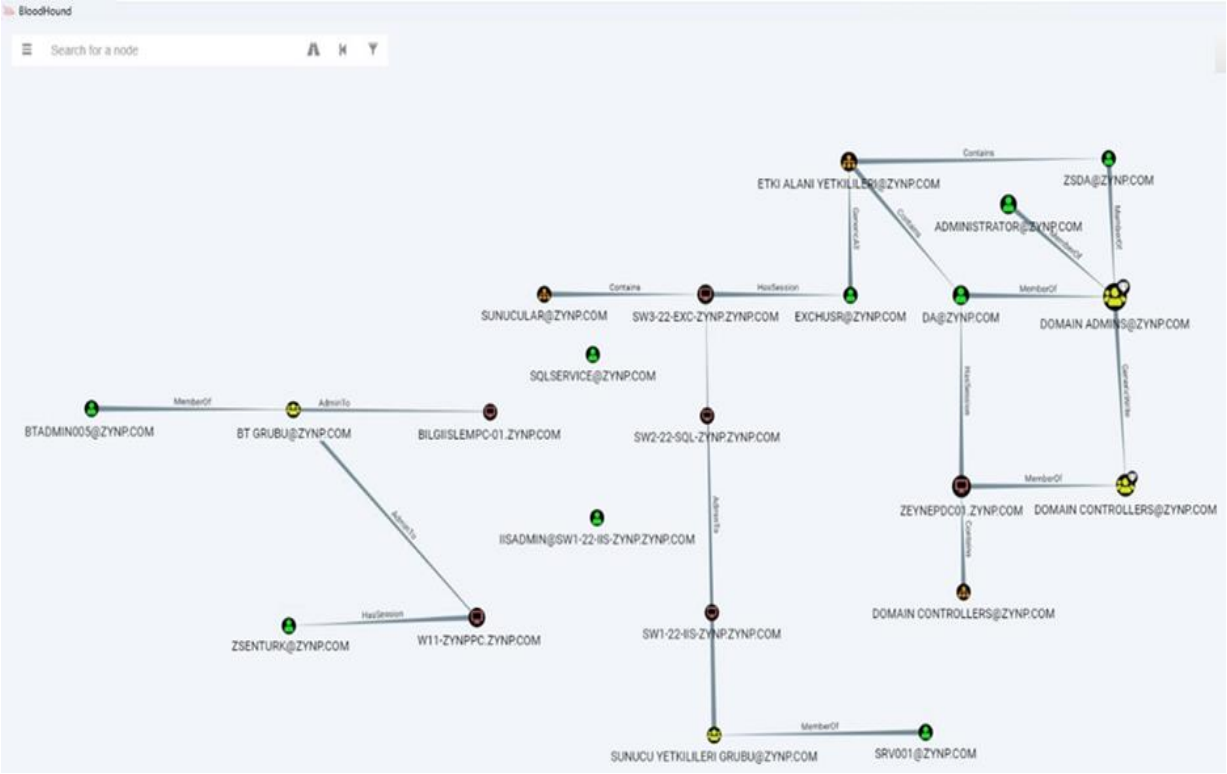
.



Şekil 2. Sızma testi senaryosu (Penetration test scenario)

3. UYGULAMA ÇALIŞMASI (EXPERIMENTAL STUDY)

Saldırgan rolündeki zsenturk@zynp.com kullanıcısının etki alanındaki kullanıcılar, gruplar ve bilgisayarlar ile ilgili ilişkileri, açık kaynaklı bir araç olan BloodHound [25] aracı ile görsel olarak Şekil 3'te sunulmuştur.



Şekil 3. Zynp.com etki alanı nesneleri arasındaki ilişkisel yapının BloodHound ile görüntülenmesi
(Visualizing the relational structure between Zynp.com domain objects with BloodHound)

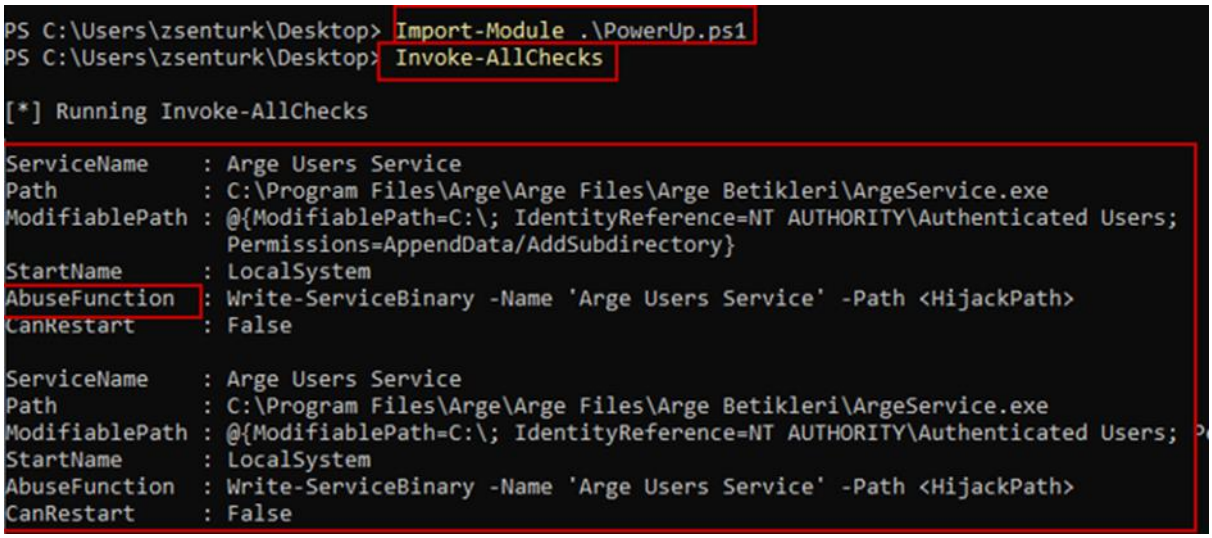
Kurumda yetkisiz bir etki alanı kullanıcısı olan zsenturk@zynp.com kullanıcısı ile W11-ZYNPPC.zynp.com bilgisayarında oturum açılmıştır. PowerShell erişimi bulunan zsenturk@zynp.com kullanıcısı ilk olarak, çalıştırılmak istenen betikler konusunda herhangi bir güvenlik sistemi tarafından engellenmemek için "Powershell.exe -ExecutionPolicy Unrestricted" parametresi kullanılarak PowerShell içerisinde yürütülecek komut veya betiklerin PowerShell tarafından kısıtlamaya uğramasını engellemiştir. Microsoft'un kötü amaçlı yazılım tespiti ve engelleme sistemini (AMSI) devre dışı bırakmak için Şekil 4'teki PowerShell komutu kullanılmıştır.

```
PS C:\Users\zsenturk\Desktop> Import-Module .\PowerView.ps1
At C:\Users\zsenturk\Desktop\PowerView.ps1:1 char:1
+ #requires -version 2
+ ~~~~~~~~~~~~~~~~~~~~
This script contains malicious content and has been blocked by your antivirus software.
    + CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent

PS C:\Users\zsenturk\Desktop> S`eT-It`em ( 'V'+'aR' +  'IA' + ('blE:1'+'q2')  + ('uZ'+'x')  ) ( [TYpE](  "{1}{0}"-F'F','rE'
 ) )  ;    (    Get-varI`A`BLE  ( ('1Q'+'2U')  +'zX'  )  -VaL  )."A`ss`Embly"."GET`TY`Pe"((  "{6}{3}{1}{4}{2}{0}{5}" -f('Uti
'+'l'),'A',('Am'+'si'),('.Man'+'age'+'men'+'t.'),('u'+'to'+'mation.'),'s',('Syst'+'em')  ) )."g`etf`iElD"(  ( "{0}{2}{1}" -f
('a'+'msi'),'d',('I'+'nitF'+'aile')  ),(  "{2}{4}{0}{1}{3}" -f ('S'+'tat'),'i',('Non'+'Publ'+'i'),'c','c,'  ))."sE`T`VaLUE"(
  ${n`ULl},${t`RuE} )
PS C:\Users\zsenturk\Desktop> Import-Module .\PowerView.ps1
PS C:\Users\zsenturk\Desktop>
```

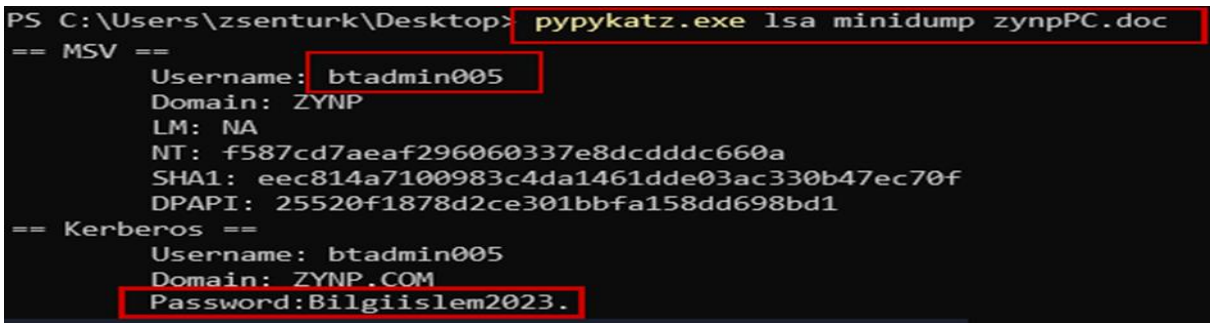
Şekil 4. AMSI Bypass için kullanılan PowerShell scripti (PowerShell script used for AMSI Bypass)

Enumeration çalışması sırasında, Şekil 5'te gösterildiği üzere "ARGE Users Service" adında hatalı yapılandırılmış bir servis tespit edilmiş ve yetkisiz kullanıcıların ilgili servis üzerinde yazma ayrıcalığı olduğu görülmüştür.



Şekil 5. PowerShell modülü ile hatalı yapılandırılmış bir servisin keşfi (Discovery of a misconfigured service with the PowerShell module)

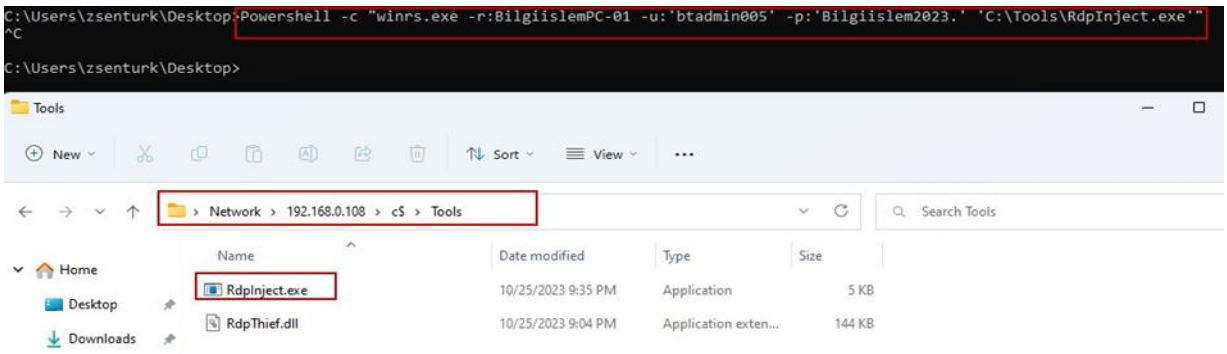
Şekil 5'te gösterilmiş olan adımda, aktif dizin zafiyetlerini sömürme aşamasında kullanılan, PowerShell tabanlı, PowerUp modülü kullanılmıştır. Bu modül ile servisin, normalde çalıştırması gereken yol (path) değiştirilerek ilgili yapılandırma hatası sömürülmüştür. Bunun sonucunda yerel bilgisayarda yetki yükseltmesi yapılmıştır. Bu yetkiye sahip olunduktan sonra zsenturk@zynp.com kullanıcısı, W11-ZYNPPC.zynp.com bilgisayarında yerel yetkili olarak oturum açmıştır. Windows güvenlik önlemleri kapatılarak atlatılmıştır. GitHub repository'de bulunan Pypycatz [26] aracı, arka planda çalıştırdığı kodlar sayesinde LSASS prosesinin belleğini doğrudan okuma yeteneğine sahiptir. Pypycatz aracı ile alınan Yerel Güvenlik Yetkilisi Alt Sistem Hizmeti (LSASS) [27] döküm dosyası analiz edilmiştir. Daha önce bu bilgisayarda oturum açmış olan btadmin05@zynp.com kullanıcısının açık metin parolası elde edilmiştir (Şekil 6).



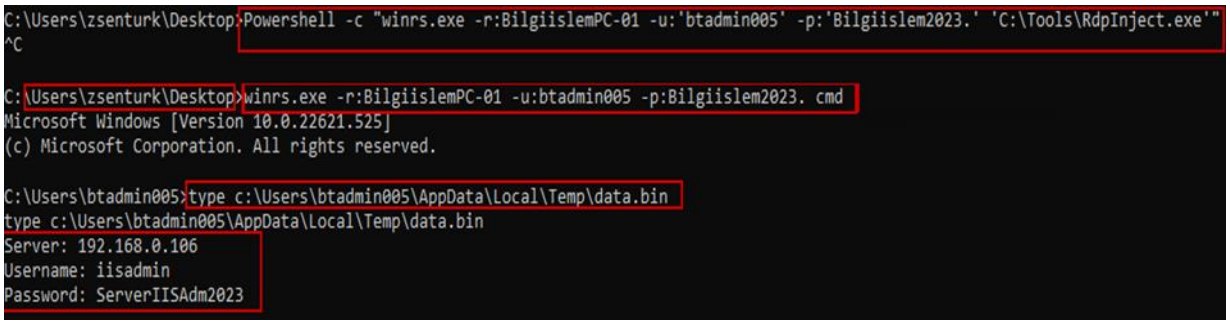
Şekil 6. LSASS döküm dosyası analizi ile btadmin005 kullanıcı bilgilerinin ele geçirilmesi (Obtaining btadmin005 user information via LSASS dump file analysis)

btadmin05@zynp.com kullanıcısı ile Find-PSRemotingLocalAdminAccess.ps1 betiği kullanılarak ağ taraması yapıldığında, BILGIISLEMPC.zynp.com bilgisayarında yerel yetkili olarak oturum açma hakkı olduğu tespit edilmiştir. Bu bilgiler ile BILGIISLEMPC.zynp.com bilgisayarında oturum açılmış fakat herhangi bir veri ele geçirilememiştir. BILGIISLEMPC.zynp.com bilgisayarına uzak bağlantı imkânı sağlayan WinRS aracılığıyla bağlantı yapılarak RDP injection saldırısı yapılmıştır. Bu saldırıda GitHub repository'de bulunan RDPCredentialStealer [28] aracı kullanılmıştır (Şekil 7).

Kullanılan aracın oluşturduğu keylogger ile hedef bilgisayar yeterli süre izlendikten sonra keylogger kayıtlarından 192.168.0.106 nolu IP ve iisadmin kullanıcı adına sahip, etki alanı üyesi olmayan bir kullanıcı ile BILGIISLEMPC.zynp.com bilgisayarına uzaktan erişim yapıldığı tespit edilmiştir (Şekil 8).

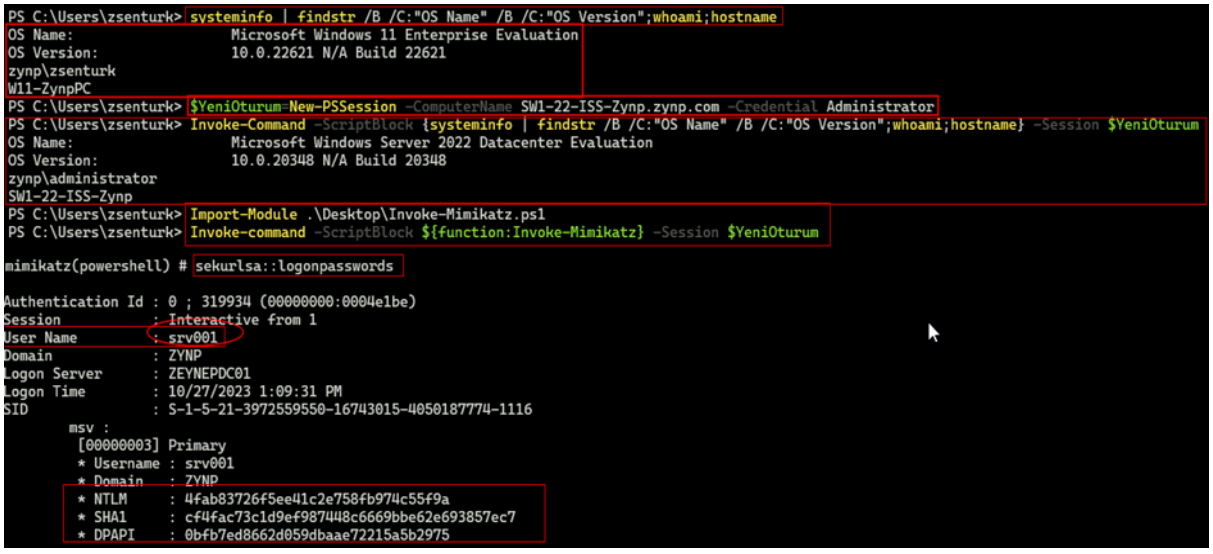


Şekil 7. RDP injection saldırısı (RDP injection attack)



Şekil 8. RDP injection sonucunda issadmin kullanıcı bilgilerinin ele geçirilmesi (Capture of issadmin user information as a result of RDP injection)

Elde edilen bilgiler ile IP bilgisi 192.168.0.106 ve adı SW1-22-ISS-ZYNP.zynp.com olan bilgisayara iisadmin yerel yetkili kullanıcısıyla erişim sağlanmıştır. SW1-22-ISS-ZYNP.zynp.com üzerinde yapılan çalışmalarda, PowerShell üzerinden Mimikatz [29] aracı kullanılarak LSASS işleminden srv001@zynp.com adlı kullanıcı ele geçirilmiştir. Mimikatz aracı, LSASS belleğinden kullanıcı bilgilerini almak için "sekurlsa::logonPasswords" komutunu kullanmaktadır. Bu komut ile yüksek yetkilerle birlikte sistem belleğindeki oturum açma kimlik bilgileri görüntülenmiş olur. srv001@zynp.com kullanıcısının etki alanı denetleyici bilgisayarları hariç ağ üzerindeki tüm üye sunucularda erişim yapabilir yetkinlikte olduğu görülmüştür (Şekil 9).

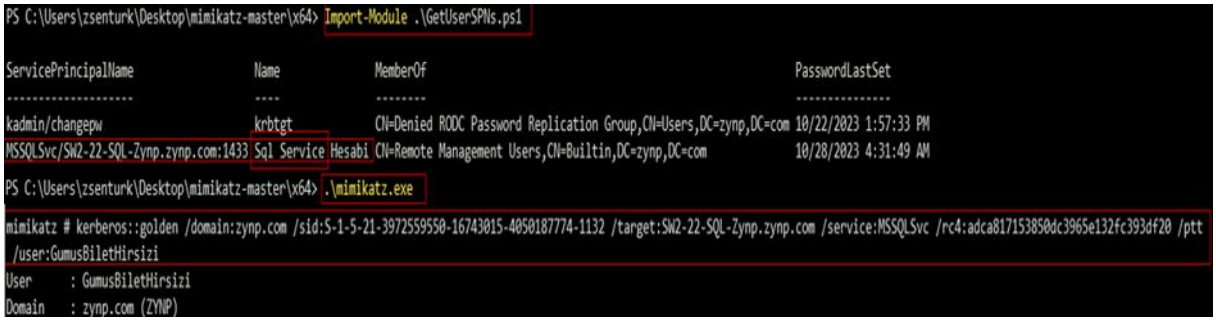


Şekil 9. SW1-22-ISS-ZYNP makinesinden srv001 kullanıcı bilgilerinin ele geçirilmesi (Obtaining user information srv001 from machine SW1-22-ISS-ZYNP

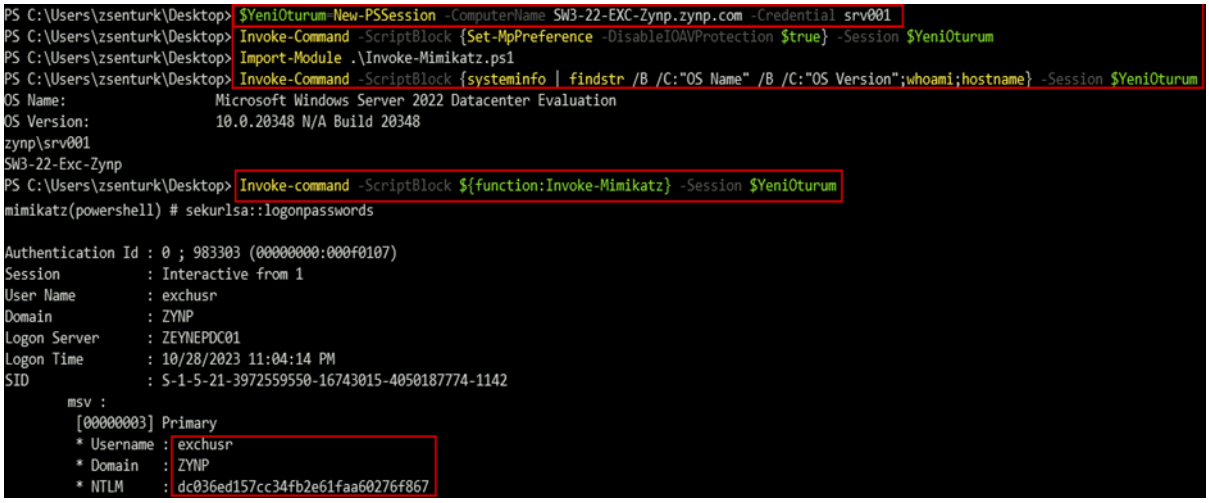
srv001@zynp.com kullanıcısı kullanılarak SW2-22-SQL-ZYNP.zynp.com bilgisayarından Mimikatz aracı ile MSSQLSvc servis hesabının parola özeti alınmıştır. Mimikatz aracı bellekteki kimlik bilgilerine erişim imkânı sunmaktadır. Bu araç ile alınan parola özeti kullanılarak yine Mimikatz aracı ile SQL servisi için gümüş bilet oluşturulmuştur (Şekil 10). Oluşturulan bu gümüş bilet sayesinde, SQL servisine sahte yetkilendirme ile kalıcı olarak (varsayılan olarak 10 yıl) erişim imkânı elde edilmiştir. Bu saldırı, sistemde kalıcılık sağlama yöntemlerinden biridir [30].

srv001@zynp.com kullanıcısı ile SW3-22-EXC-ZYNP.zynp.com sunucu bilgisayarına da erişim yapılmıştır. Bu bilgisayara erişim yapılarak exchusr@zynp.com kullanıcısı ele geçirilmiştir (Şekil 11).

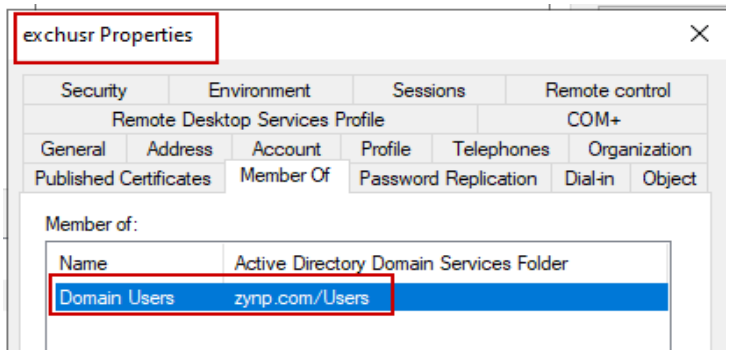
Kullanıcıyla ilgili yapılan incelemede, exchusr@zynp.com kullanıcısının etki alanındaki mevcut rolünün standart kullanıcı olduğu Şekil 12'de gösterildiği gibi tespit edilmiştir.



Şekil 10. SQL servisi için Mimikatz aracı ile Gümüş Bilet oluşturulması (Creating a Silver Ticket with Mimikatz tool for SQL service)



Şekil 11. SW3-22-EXC-ZYNP makinesinden exchuser kullanıcı bilgilerinin ele geçirilmesi (Obtaining exchuser user information from machine SW3-22-EXC-ZYNP)



Şekil 12. exchusr kullanıcısının etki alanındaki rolünü gösterir ekran resmi (Screenshot showing the role of user exchusr in the domain)

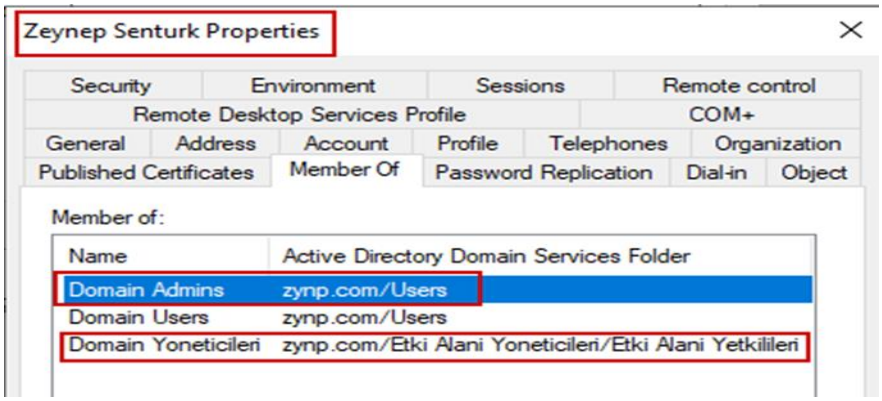
Eski bir etki alanı yönetici grubu üyesi olduğu kullanıcı açıklamasında yazan exchusr@zynp.com kullanıcısının, tüm yetkilerinin alındığı fakat "Domain Yöneticileri" adlı bir kullanıcı grubunun Erişim Kontrol Listesi (ACL)'sinde "Generic All" ayrıcalığına sahip olduğu tespit edilmiştir (Şekil 13). "Domain Yöneticileri" grubu incelendiğinde "Domain Admins" grubuna üye bir grup olduğu tespiti yapılmıştır.

Bu özellik exhuser sayesinde sömürülerek başlangıçta standart yetkilere sahip olan zsenturk@zynp.com kullanıcısı, önce "Domain Yöneticileri" grubuna daha sonra "Domain Admins" grubuna üye yapılmıştır (Şekil 14).

"Domain Yöneticileri" grubu, aktif dizin ortamında yerleşik olarak gelen "Domain Admins" grubunun üyesi olduğundan zsenturk@zynp.com kullanıcısı "Domain Admins" grubuna üye yapılmasa dahi etki alanı denetleyicisinde oturum açabilen bir konuma gelmiştir. Bu adım ile kurumda yetkisiz bir kullanıcı olan zsenturk@zynp.com kullanıcısı, nihai hedefi olan kurumun en yetkili bilgisayarına erişim elde etmiştir.

```
PS C:\Users\zsenturk\Desktop> Find-InterestingDomainAcl -ResolveGUIDs
WARNING: [Find-InterestingDomainAcl] Unable to convert SID 'S-1-5-21-3972559550-16743015-4050187774-1141' to a distinguishedname
ObjectDN                : CN=Exchange Olusturma Kullanicisi,OU=Etki Alani Yetkilileri,OU=Etki Alani Yoneticileri,DC=zynp,DC=com
AceQualifier            : AccessAllowed
ActiveDirectoryRights   : GenericAll
ObjectAceType           : All
AceFlags                : ContainerInherit, Inherited
AceType                 : AccessAllowedObject
InheritanceFlags        : ContainerInherit
SecurityIdentifier      : S-1-5-21-3972559550-16743015-4050187774-1142
IdentityReferenceName   : exchusr
IdentityReferenceDomain : zynp.com
IdentityReferenceDN     : CN=Exchange Olusturma Kullanicisi,OU=Etki Alani Yetkilileri,OU=Etki Alani Yoneticileri,DC=zynp,DC=com
IdentityReferenceClass  : user
```

Şekil 13. ACL kontrolü sonucu exchusr kullanıcısının "Generic All" ayrıcalığının keşfi (Discovery of exchusr user's "Generic All" privilege as a result of ACL check)



Şekil 14. exchusr kullanıcısının Domain Yöneticileri grubuna eklenmesi (Adding exchusr to the Domain Administrators group

4. DEĞERLENDİRME ve ÖNERİLER (EVALUATION AND RECOMMENDATIONS)

Çalışma sonucunda; örnek kurumsal ağda PowerShell erişimine sahip yetkisiz bir kullanıcının, sistemdeki çeşitli yapılandırma hatalarından yararlanarak etki alanının en yetkili bilgisayarı olan etki alanı kontrolcüsüne erişebilir hale geldiği görülmüştür. Bu durum, kurumlar için oldukça kritik bir güvenlik sorundur. Çünkü bu durum ağdaki erişim kontrolü kaybını temsil eder. Erişim kontrolü, belirli kullanıcıların belirli kaynaklara erişimini kısıtlamak için kullanılan bir güvenlik önlemidir. Yetkisiz erişim ile hassas verilere ve kaynaklara yetkisiz erişim sağlanabilir, bu da bilgi sızıntısı, veri kaybı veya kötü niyetli faaliyetler gibi ciddi sonuçlara yol açabilir. Bir saldırganın etki alanı kontrolcüsüne erişimi, kuruluşun tüm kullanıcı hesaplarına, grup politikalarına, güvenlik ayarlarına ve diğer kritik bilgilere erişim sağlar. Bu, saldırganın kuruluşun tüm ağını kontrol etmesine ve hatta tamamen devralmasına olanak tanır. Saldırgan, kullanıcı hesaplarını değiştirebilir, yetkilendirmeleri değiştirebilir, hassas verilere erişebilir veya hatta sistemleri devre dışı bırakabilir. Bu tür faaliyetler, kuruluşun faaliyetlerini durdurabilir veya ciddi veri kayıplarına neden olabilir. Öte yandan etki alanı kontrolcüsüne erişim, saldırganın bir kuruluşun tamamını hedefleyen koordineli ve dağıtılmış saldırılar başlatmasına olanak tanır. Bu, bir saldırganın kuruluşun bütününü hedef alarak daha geniş çaplı ve yıkıcı sonuçlar doğurabilecek bir saldırı düzenlemesine imkân sağlar.

Saldırıların her zaman için dışarıdan geleceği kanısı doğru değildir. Bazen saldırgan kişiler, sistemin teslim edildiği kişiler de olabilir. Bu sebeple, sistemlerin kişilerden bağımsız olarak güvenli bir şekilde yapılandırılması gerekmektedir. Bu saldırılardan korunmak amacıyla alınabilecek temel önlemler aşağıda sıralanmıştır:

- Kurumsal ağlarda, sistemleri daha güvenli hale getirmek için kullanıcıların kabuk katmanı erişimi engellenmelidir. Sunucu bilgisayarların kayıtları düzenli bir şekilde tutulmalı ve izlenmelidir. Gereksiz servisler, bilgi ifşaları ve zafiyet oluşturma ihtimallerinin önüne geçmek için kapatılmalıdır.

- Etki alanındaki bilgisayarlara, güvenlik riski oluşturduklarından dolayı, yerel yetkili kullanıcılar erişim sağlayamamalıdır. Sistemde, yerel yetkili kullanıcıların olması gerektiği durumda ise bu kullanıcılar kesinlikle ortak kullanıcı olarak kullanılmamalıdır. Sistemi daha güvenli hale getirmek için etki alanı yetkilendirmelerinde katmanlı güvenlik mimarisi uygulanmalıdır.
- Sistemler üzerinde yetkili kullanıcı hesabı olmak zorunda olan kurum çalışanları için yetkilendirme yapılarına göre iki veya üç kullanıcı hesabı tanımlanması tavsiye edilmektedir. Yetkili kullanıcı hesaplarının, sistemleri yönetmek için olduğu unutulmamalı ve asla rutin işler için kullanılan bilgisayarlara bu hesaplar ile erişilmemelidir.
- Sistemde yapılan tüm güvenlik yapılandırmaları, etki alanı kontrolcüsünden grup ilkesi olarak uygulanmalıdır. Etki alanı üyesi bilgisayarlarda oturum açan kullanıcıların yetkilendirmeleri, son derece hassas bir şekilde yapılandırılmalıdır. Kullanıcılar, her zaman en az ayrıcalığa sahip olacak şekilde yetkilendirilmelidir. Erişilecek servisler, kısayollar veya sistem dosyaları gibi hassas yerler dikkatlice korunmalıdır.
- Organizasyonların; oluşturdukları bilgi güvenliği politikalarını güncel ihtiyaçlar doğrultusunda belirli periyotlarda değiştirmeleri tavsiye edilmektedir. Sızma testlerinde tespit edilemeyen güvenlik açıklıklarının olabileceği göz önünde bulundurularak, her sızma testi sonrasında, etki alanı sıkılaştırmalarının organizasyon yapısına uygun şekilde gözden geçirilmesi, sistem güvenliğine önemli katkı sağlayacaktır. Sızma testleri, güvenlik sıkılaştırmaları ve zafiyet taramaları belirli periyotlarda düzenli olarak yapılmalıdır. Sistemlerde, güncellemeleri devam eden yazılımların kullanılması ve güncellemelerin düzenli bir şekilde test edilerek yapılması tavsiye edilmektedir.

- Bu önlemlere ek olarak, kurumlarda fiziksel güvenlik önlemlerinin çok sıkı bir şekilde uygulanması tavsiye edilmektedir. Alınabilecek fiziksel güvenlik önlemleri sayesinde, işletim sisteminde yetki yükseltme işlem basamağının önüne geçilebilir. Fiziksel güvenlik ile kurumsal veya kişisel verilerle ilgili donanımsal olarak veri kaybı riski azaltılabilir.

5. SONUÇ (CONCLUSION)

Bu çalışma, Windows Aktif Dizin Etki Alanı Servisi'nin kurumsal ağ güvenliği açısından önemini ve PowerShell erişiminin potansiyel tehlikelerini ele almıştır. Gerçekleştirilen sızma testi, yetkisiz bir kullanıcının PowerShell aracılığıyla etki alanında ciddi güvenlik açıkları yaratabileceğini ve en yetkili bilgisayara erişim sağlayabileceğini göstermiştir. Bu durum, kurumlar için ciddi bir güvenlik riski oluşturmaktadır. Çalışmanın bulguları, kurumsal ağlarda PowerShell erişimine sahip kullanıcıların yetkilerinin dikkatlice kontrol edilmesi gerektiğini vurgulamaktadır. Ayrıca, sistemlerin yapılandırılmasında katmanlı güvenlik mimarisi kullanılması, yerel yetkili kullanıcıların erişimlerinin kısıtlanması ve güvenlik politikalarının düzenli olarak gözden geçirilmesi önemlidir. Düzenli olarak yapılan sızma testleri ve güncellemelerin düzenli bir şekilde uygulanması, kurumların güvenlik seviyelerini artırmada kritik öneme sahiptir. Çalışmada önerilen önlemlerin uygulanmasıyla, kurumlar yetkisiz erişimlerin önüne geçebilir ve güvenliklerini artırabilirler. Fiziksel güvenlik önlemlerinin de dikkate alınması, kurumların veri kaybı riskini azaltabilir ve güvenliklerini daha da sağlamlaştırabilir. Çalışmanın, kurumsal ağ güvenliği alanında farkındalığın artırılmasına ve kurumların daha güvenli bir dijital ortam oluşturmalarına katkılar sağlayacağı değerlendirilmiştir.

ETİK STANDARTLARIN BEYANI
(DECLARATION OF ETHICAL STANDARDS)

Bu makalenin yazarı çalışmalarında kullandıkları materyal ve yöntemlerin etik kurul izni ve/veya yasal-özel bir izin gerektirmediğini beyan ederler.

The author of this article declares that the materials and methods they use in their work do not require ethical committee approval and/or legal-specific permission.

YAZARLARIN KATKILARI (AUTHORS' CONTRIBUTIONS)

Zeynep ŞENTÜRK ve Erdal IRMAK: Bu çalışmada yazarlar eşit katkı sağlamıştır.

The authors contributed equally to this study.

ÇIKAR ÇATIŞMASI (CONFLICT OF INTEREST)

Bu çalışmada herhangi bir çıkar çatışması yoktur.

There is no conflict of interest in this study.

KAYNAKLAR (REFERENCES)

[1] Market share held by the leading computer (desktop/tablet/console) operating systems worldwide from January 2012 to January 2023, https://www.statista.com/statistics/268237/global-market-share-held-by-operating-systems-since-2009/

[2] Grillenmeier, G., Now's the time to rethink Active Directory security, Network Security, No. 7, (2021) 13-16.

[3] Kaspersky IT Security Economics, 2022. https://go.kaspersky.com/rs/802-IJN-240/images/IT%20Security%20Economics%202022_report.pdf

[4] Biggest Insider Threats of 2022: Lessons Learned and Key Takeaways for 2023, https://www.computer.org/publications/tech-news/trends/key-takeaways-from-2022-cyberthreatseaways-for-2023

[5] The 2019 Insider Threat Report, https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/insider-threat-report.pdf

[6] Microsoft mitigated exposure of internal information in a storage account due to overly-permissive SAS token, https://msrc.microsoft.com/blog/2023/09/microsoft-mitigated-exposure-of-internal-information-in-a-storage-account-due-to-overly-permissive-sas-token/

[7] Tesla sues ex-employee for hacking, theft, and leaking to the press, https://www.theverge.com/2018/6/20/17484030/tesla-sues-employee-hacking-theft-leaking

[8] Vishnuram, G., Tripathi, K., & Tyagi, A. K., Ethical Hacking: Importance, Controversies and Scope in the Future, IEEE International Conference on Computer Communication and Informatics, Coimbatore, (2022) 01-06.

[9] Mokhtar, B. I., Jurcut, A. D., ElSayed, M. S., & Azer, M. A., Active Directory Attacks-Steps, Types, and Signatures, Electronics, 11 No. 16 (2022) 2629-2652.

[10] Bertoglio, D. D., & Zorzo, A. F., Overview and open issues on penetration test, Journal of the Brazilian Computer Society, 23 No. 2 (2017) 1-16.

[11] Use Alternate Authentication Material: Pass the Hash, MITRE ATT&CK, https://attack.mitre.org/techniques/T1550/002/

[12] Steal or Forge Kerberos Tickets, MITRE ATT&CK, https://attack.mitre.org/techniques/T1558/

[13] What is PowerShell?, https://learn.microsoft.com/en-us/powershell/scripting/overview?view=powershell-7.4.

[14] Aiello, J., PowerShell Core 6.0: Generally Available (GA) and Supported!, https://devblogs.microsoft.com/powershell/powershell-core-6-0-generally-available-ga-and-supported/

[15] Tigner, M., Wimmer, H., & Rebman, C. M. Analysis of Kali Linux Penetration Tools: A Survey of Hacking Tools, International Conference on Electrical, Computer and Energy Technologies, (2021) 1-6

[16] Raj, S., & Walia, N. K., A Study on Metasploit Framework: A Pen-Testing Tool, IEEE International Conference on Computational Performance Evaluation (ComPE), (2020) 296-302.

[17] Shah, M., Ahmed, S., Saeed, K., Junaid, M., Khan, H., & Ata-ur-Rehman., Penetration Testing Active Reconnaissance Phase – Optimized Port Scanning With Nmap Tool, IEEE 2nd International Conference on Computing, Mathematics and Engineering Technologies, (2019) 1-6.

[18] Liao, S., Zhou, C., Zha, Y., Zhang, Z., Zhang, C., Gao, Y., & Zhong, G., Comprehensive Detection Approach of Nmap: Principles, Rules and Experiments Attack Detection based on Domain Attack Behavior Analysis, IEEE International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, (2020).

[19] Rozendaal, K., & Mailewa, A. B., A Novel Method for Moving Laterally and Discovering Malicious Lateral Movements in Windows Operating Systems: A Case Study, Advances in Science and Technology, 2, No. 3, (2022) 291-321.

[20] Aibekova, A., & Selvarajah, V., Offensive Security: Study on Penetration Testing Attacks, Methods, and Their Types, IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics, (2022) 1-9.

[21]Advanced Infrastructure Penetration Testing: Defend your systems from methodized and proficient attackers,https://books.google.com.tr/books?hl=tr&lr=&id=BulODwAAQBAJ&oi=fnd&pg=PP1&dq=pentest+with+powershell&ots=W5iD8S8wry&sig=FNT9erdlvKoVL9Y2emLFyLq4RqI&redir_esc=y#v=onepage&q=pentest%20with%20powershell&f=false

[22] Infrastructure Penetration Testing,

https://web.archive.org/web/20230310233435id_/http://ikee.lib.auth.gr/record/345496/files/GRI-2023-38338.pdf

[23] NIST Technical Guide to Information Security Testing and Assessment, NIST, 09 2008. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf.

[24] VMware Workstation Pro, https://www.vmware.com/products/workstation-pro.html.

[25] BloodHoundAD, GitHub, https://github.com/BloodHoundAD/BloodHound.

[26] skelsec/pypykatz, GitHub, https://github.com/skelsec/pypykatz.

[27] Configure added LSA protection, Microsoft, https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection

[28]RDPCredentialStealer,S12cybersecurity, https://github.com/S12cybersecurity/RDPCredentialStealer/tree/main/RDPCredsStealerDLL/RDPCredsStealerDLL.

[29] ParrotSec/Mimikatz, GitHub,https://github.com/ParrotSec/mimikatz.

[30] Motero, C. D., Hıguera, J. R. B., Hıguera, J. B., Montalvo, J. A. S., & Gómez, N. G., On Attacking Kerberos Authentication Protocol in Windows Active Directory Services: A Practical Survey, IEEE Access, 9, (2021) 09289-109319.