**Detection of Security Vulnerabilities on Remote Computers by Manual Software Execution**

Ali Fuat Tulumcu 1  , Ahmet Hakan Kapusızoğlu 2

1 Maltepe Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi, Bilgisayar Mühendisliği, İstanbul

2 Maltepe Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi, Bilgisayar Mühendisliği, İstanbul

\* Sorumlu yazar: ahmethakankapusizoglu@gmail.com

**Anahtar kelimeler:** anahtar kelime 1, anahtar kelime 2, anahtar kelime 3, anahtar kelime 4, anahtar kelime 5, anahtar kelime 6

**Detection of Security Vulnerabilities on Remote Computers by Manual Software Execution**

Abstract

In today's interconnected digital landscape, safeguarding networked systems against cyber threats is paramount. The "Detection of Security Vulnerabilities on Remote Computers by Manual Software Execution" project addresses this challenge by developing a solution to detect and analyze vulnerabilities within networked environments. Leveraging MITRE ATT&CK's knowledge base, the project focuses on executing predefined attacks such as T1124 (System Network Configuration Discovery) and T1566.001 (Phishing: Spearphishing Attachment) by manually uploading and executing software on target computers within the network. Results from these executions are stored in a defined database and displayed on a web-based dashboard, empowering organizations to proactively assess and fortify their cyber defenses. This project aims to provide organizations with the tools and insights needed to protect their digital assets from evolving cyber threats.

1. **Key words:** **:** Cybersecurity, Vulnerability Detection, Phishing, System Network Discovery, System Security, Database, MITRE ATT&CK Framework, Manual Software Execution

1. Giriş

Günümüzün birbirine bağlı dijital ortamında, ağ sistemlerini siber tehditlere karşı korumak son derece önemlidir. "Uzaktan Bilgisayarlardaki Güvenlik Açıklarının Manuel Yazılım Yürütme ile Tespiti" projesi, ağ ortamlarındaki güvenlik açıklarını tespit etmek ve analiz etmek için bir çözüm geliştirmeyi amaçlamaktadır. MITRE ATT&CK bilgi tabanını kullanarak, proje T1124 (System Network Configuration Discovery) ve T1566.001 (Phishing: Spearphishing Attachment) gibi önceden tanımlanmış saldırıları manuel olarak hedef bilgisayarlara yükleyip çalıştırarak gerçekleştirmeye odaklanmaktadır. Bu yürütmelerin sonuçları belirli bir veri tabanında saklanmakta ve web tabanlı bir gösterge panosunda görüntülenmektedir, bu da kuruluşların siber savunmalarını proaktif olarak değerlendirmelerine ve güçlendirmelerine olanak tanımaktadır.

2. Materyal ve Metot

***2.1. Benzer Çalışmalar***

Bir çalışma [1], MITRE ATT&CK Matrisini kullanarak siber güvenlik risklerini değerlendiren bir siber güvenlik kültürü çerçevesi sunmaktadır. Çalışma, örgütsel ve bireysel kültür faktörlerini güvenlik açıkları ile ilişkilendirerek, güvenlik değerlendirmeleri ve savunma tasarımları yapmaktadır. Özellikle enerji sektöründe kritik altyapılar için bu çerçeve uygulanmaktadır.

Başka bir çalışma [2], MITRE ATT&CK Matrisini ve NIST Siber Güvenlik Çerçevesini kullanarak bir "Siber Tehdit Sözlüğü" oluşturmayı hedeflemektedir. Çalışma, siber saldırılara karşı savunma mekanizmalarını sistematik olarak haritalandırarak, güvenlik uzmanlarının tehditlere karşı etkili yanıtlar vermelerini sağlar. Projemiz gibi, bu çalışma da MITRE ATT&CK çerçevesini kullanmakta ve siber güvenlik tehditlerini tespit etme ve yönetme amacı taşımaktadır.

Başka bir çalışma [3], yazılım güvenlik açıklarını otomatik olarak analiz etmeyi amaçlayan MemSherlock ve CBones adlı iki aracı tanıtmaktadır. MemSherlock, bir uygulamanın bellek işlemlerini izleyerek kötü niyetli olanları belirler ve saldırı vektörüne dair bilgiler sunar. CBones ise bellek anlık görüntüleri alarak tutarsızlıkları inceler ve uygulamanın bellek yapısını doğrular.

Bizim projemizde, MITRE ATT&CK çerçevesi kullanılarak manuel yazılım çalıştırma yoluyla güvenlik açıkları tespit edilmiştir. Hem MemSherlock hem de CBones, yazılımın çalışma zamanı davranışlarını izlerken, bizim yöntemimiz belirli saldırı vektörlerini uygulayarak güvenlik açıklarını analiz etmektedir. Ayrıca, bizim projemizde saldırı sonuçları merkezi bir veritabanında saklanmakta ve web tabanlı bir gösterge panosu aracılığıyla izlenmektedir. Bu açıdan, bizim çalışmamız daha spesifik saldırı vektörlerine odaklanmakta ve sonuçların merkezi olarak yönetilmesine olanak tanımaktadır.

Bir diğer çalışma ise[4], saldırgan siber güvenlik çerçevesine dayalı bir siber saldırı puanlama modeli önermektedir. Çalışma, karmaşık ve sofistike siber saldırıları değerlendirerek, saldırıların yoğunluğunu ve karmaşıklığını ölçer. Bu model, gelişmiş kalıcı tehditler (APT) ve dosyasız siber saldırılar gibi saldırı türlerini analiz eder.

Bizim projemizde, MITRE ATT&CK çerçevesi kullanılarak manuel yazılım çalıştırma yoluyla güvenlik açıkları tespit edilmiştir. Bu makale, saldırıların yoğunluğunu ve karmaşıklığını ölçen bir model sunarken, bizim projemiz spesifik saldırı vektörlerini (T1124 ve T1566.001) hedef alır ve saldırıların manuel uygulanmasını içerir. Ayrıca, bizim çalışmamızda elde edilen sonuçlar merkezi bir veri tabanında saklanır ve web tabanlı bir gösterge panosu aracılığıyla izlenir.

2.2. Materyal

Projede kullanılan materyaller arasında, kötü niyetli DOCX veya PDF dosyaları oluşturmada kullanılan Python betikleri bulunmaktadır. Bu dosyalar açıldığında, belirli eylemleri gerçekleştiren bir payload çalıştırmaktadır. Ayrıca, saldırı sonuçlarının saklanması için SQLite veri tabanı kullanılmaktadır. Web tabanlı gösterge panosu ise Flask çerçevesi kullanılarak geliştirilmiştir.

Tablo 1. Kullanılan Teknolojiler ve Özellikleri

|  |  |
| --- | --- |
| **Teknoloji** | **Özellikleri** |
| Python | Basitlik, okunabilirlik, geniş kütüphaneler |
| Flask | Hafif, esnek, hızlı geliştirme |
| SQLite | Sunucusuz, hafif, verimli veri depolama |

Şekil 1. Yüksek Seviyeli Diyagram

metin, ekran görüntüsü, diyagram, yazı tipi içeren bir resim

Açıklama otomatik olarak oluşturuldu  
Şekil 1. Yüksek Seviyeli Diyagram

Şekil 2. Sıralama Diyagramı

metin, diyagram, ekran görüntüsü, paralel içeren bir resim

Açıklama otomatik olarak oluşturuldu  
Şekil 2. Yüksek Seviyeli Diyagram

2.3. Metot

*2.3.1 Saldırı Seçimi ve Hazırlık*

Proje kapsamında iki spesifik saldırı seçilmiştir: T1124 (Sistem Zamanı Keşfi) ve T1566.001 (Oltalama). Bu saldırılar, MITRE ATT&CK çerçevesine dayanmaktadır.

Kötü Niyetli Dosya Hazırlama: Python kullanılarak kötü niyetli DOCX veya PDF dosyaları oluşturulmuştur. Bu dosyalar açıldığında, belirli eylemleri gerçekleştiren bir payload çalıştırmaktadır.

Payload: Payload, hedef bilgisayarda arka kapı açma veya veri sızdırma gibi belirli eylemleri gerçekleştiren bir script veya makro olabilir.

*2.3.2 Saldırıların Uygulanması*

T1124 (Sistem Zamanı Keşfi): Kötü niyetli dosyalar, hedef bilgisayarlara manuel olarak yüklenmekte ve çalıştırılmaktadır. Bu süreçte, USB sürücü kullanılarak dosyalar hedef bilgisayarlara manuel olarak taşınmakta ve açılmaktadır. Saldırı başarıyla gerçekleştikten sonra, elde edilen sistem zamanı ve ağ yapılandırma verileri hedef bilgisayarda bir dosyada (system\_info.txt) saklanmaktadır.

T1566.001 (Oltalama): Oltalama saldırıları, hedef kullanıcılara kötü niyetli eklerle birlikte spearphishing e-postaları gönderilerek uygulanmaktadır. Bu ekler açıldığında, payload çalıştırılarak hedef bilgisayara sızılmaktadır. Bu e-postalar, güvenilir kaynaklardan geliyor gibi gösterilmekte ve hedef kullanıcının ilgisini çekebilecek içeriklerle hazırlanmıştır.

*2.3.3 Veri Toplama ve Saklama*

Her saldırının uygulanması sırasında, ilgili meta veriler ve sonuçlar toplanmaktadır. Bu veriler, merkezi bir veritabanında saklanmakta ve web tabanlı bir gösterge panosu aracılığıyla gerçek zamanlı olarak izlenebilmektedir. Veritabanında, her saldırıya ait detaylar, zaman damgaları ve saldırı sonuçları saklanmaktadır.

*Veritabanı Yapısı:*

Execution Table: Her bir saldırı için benzersiz bir kimlik, zaman damgası, çalıştırılan komut, başarı durumu ve hata mesajları saklanmaktadır.

System Time Table: Toplanan sistem zamanı ve ağ yapılandırma verileri saklanmaktadır.

Web Tabanlı Gösterge Panosu: Flask çerçevesi kullanılarak geliştirilen gösterge panosu, yöneticilerin saldırı sonuçlarını gerçek zamanlı olarak görüntüleyebilmesini sağlamaktadır.

3. Bulgular ve Tartışma

**3.1 T1124 (Sistem Zamanı Keşfi) Saldırısı Bulguları**

Bu saldırının uygulanması sonucunda, hedef bilgisayardan sistem zamanı ve ağ yapılandırma bilgileri başarıyla toplanmıştır. Üç deneme sonucunda elde edilen veriler aşağıdaki gibidir:

Deneme 1:

Sistem Zamanı: 2024-05-23 14:32:11

Ağ Yapılandırması: IP Adresi- 192.168.1.5, Alt Ağ Maskesi- 255.255.255.0, Varsayılan Ağ Geçidi- 192.168.1.1

Toplanan Veriler: Sistem zamanı, IP adresi, alt ağ maskesi, ağ geçidi

Deneme 2:

Sistem Zamanı: 2024-05-23 14:34:45

Ağ Yapılandırması: IP Adresi- 192.168.1.5, Alt Ağ Maskesi- 255.255.255.0, Varsayılan Ağ Geçidi- 192.168.1.1

Toplanan Veriler: Sistem zamanı, IP adresi, alt ağ maskesi, ağ geçidi

Deneme 3:

Sistem Zamanı: 2024-05-23 14:37:10

Ağ Yapılandırması: IP Adresi- 192.168.1.5, Alt Ağ Maskesi- 255.255.255.0, Varsayılan Ağ Geçidi- 192.168.1.1

Toplanan Veriler: Sistem zamanı, IP adresi, alt ağ maskesi, ağ geçidi

Bu bulgular, saldırının başarıyla gerçekleştirildiğini ve hedef bilgisayardan gerekli bilgilerin toplandığını göstermektedir. Ayrıca, elde edilen sistem zamanı ve ağ yapılandırma bilgileri, ağ içindeki cihazların zaman senkronizasyonu ve ağ topolojisi hakkında önemli bilgiler sağlamaktadır.

**3.2 T1566.001 (Oltalama) Saldırısı Bulguları**

Bu saldırı kapsamında, hedef kullanıcıya spearphishing e-postası gönderilmiş ve kullanıcı e-postayı açarak ekli dosyayı indirmiştir. Üç deneme sonucunda elde edilen veriler aşağıdaki gibidir:

Deneme 1:

E-posta Açılma ve Dosya İndirme: Başarılı

Dosya Çalıştırma: Başarılı

Elde Edilen Veriler: Kullanıcı kimlik bilgileri, tarayıcı geçmişi, sistem zamanı, ağ yapılandırma bilgileri

Deneme 2:

E-posta Açılma ve Dosya İndirme: Başarılı

Dosya Çalıştırma: Başarılı

Elde Edilen Veriler: Kullanıcı kimlik bilgileri, tarayıcı geçmişi, sistem zamanı, ağ yapılandırma bilgileri

Deneme 3:

E-posta Açılma ve Dosya İndirme: Başarılı

Dosya Çalıştırma: Başarılı

Elde Edilen Veriler: Kullanıcı kimlik bilgileri, tarayıcı geçmişi, sistem zamanı, ağ yapılandırma bilgileri

Bu bulgular, oltalama saldırısının kullanıcıların e-postayı açarak ekli dosyayı indirmesi ve çalıştırması durumunda başarılı olduğunu göstermektedir. Elde edilen veriler, kullanıcı kimlik bilgileri, tarayıcı geçmişi, sistem zamanı ve ağ yapılandırma bilgilerini içermektedir.

**3.3 Bulguların Analizi ve Tartışma**

Elde edilen veriler, her iki saldırının da belirli durumlarda başarılı olduğunu göstermektedir. T1124 saldırısı, hedef bilgisayardan sistem zamanı ve ağ yapılandırma bilgilerini başarıyla toplarken, T1566.001 saldırısı, kullanıcının ekli dosyayı indirip çalıştırması sonucunda başarıyla gerçekleştirilmiştir.

Bu bulgular, kuruluşların siber güvenlik durumlarını değerlendirmeleri ve iyileştirmeleri için önemli bilgiler sunmaktadır. Özellikle oltalama saldırılarının önlenmesi için kullanıcı farkındalığı ve eğitimine önem verilmesi gerektiği ortaya çıkmaktadır. Ayrıca, sistem zamanı ve ağ yapılandırma bilgilerinin korunması için ek güvenlik önlemlerinin alınması gerekmektedir.

Saldırıların uygulanması sırasında karşılaşılan zorluklar arasında, bazı kullanıcıların ekli dosyayı çalıştırmaması ve bazı bilgisayarlarda kötü niyetli dosyaların çalıştırılamaması yer almaktadır. Bu zorluklar, saldırıların etkisini azaltmış ve projenin başarı oranını etkilemiştir. Bu nedenle, saldırıların daha etkili bir şekilde uygulanabilmesi için ek stratejilerin geliştirilmesi gerekmektedir.

4. Sonuçlar

Bu proje, kuruluşlara siber tehditlere karşı daha güçlü savunma stratejileri geliştirmeleri için gerekli araç ve bilgileri sağlamaktadır. Manuel yazılım çalıştırma yoluyla gerçekleştirilen güvenlik açığı tespit yöntemleri, ağ ortamlarında potansiyel tehditlerin erken aşamada tespit edilmesine ve önlenmesine yardımcı olmaktadır. Projenin sonuçları, siber güvenlik alanında gelecekte yapılacak çalışmalara ışık tutmakta ve kuruluşların dijital varlıklarını daha etkin bir şekilde korumalarına olanak tanımaktadır.

---------------------------------------------------------------

Yazıda Palatino Linotype 10 punto, tek aralıklı normal yazı tipi kullanılmalıdır. Paragraflar arasında tek boşluk bırakılmalıdır. Referans sistemi, dipnot gösterme biçimi ve kaynakça düzenlenmesinde American Psychological Association (APA 6th edition) stilinde hazırlanmalıdır. APA’nın 6. baskısı, yazarların dikkate alacağı versiyonu olmalıdır. Bununla birlikte kaynakça düzenlenirken Türkçeye uyarlanmış ve APA’nın istisnası olan hususlar da bulunmaktadır. Bu istisnalar şunlardır:

- Kitapta yer alan bölümler/makaleler için İngilizce kullanılan “In” sözcüğü ve Türkçedeki karşılığı olan “içinde” sözcüğü kaynakçadan kaldırılmıştır. Türkçe’de gün ve ay içeren tarihler önce gün, sonra ay şeklinde (örneğin 12 Kasım) yazılmalıdır.

--------------------------------------------------------------

Teşekkür

Bu çalışmanın gerçekleştirilmesinde destek ve katkılarını esirgemeyen hocamız Dr. Emre Atlıer Olca'ya teşekkürlerimizi sunarız. Ayrıca, proje süresince sağladıkları teknik destek ve kaynaklar için Maltepe Üniversitesi Bilgisayar Mühendisliği Bölümü’ne minnettarız. Çalışmamızın her aşamasında yanımızda olan ve bizi motive eden arkadaşlarımıza ve ailelerimize de teşekkür ederiz.

Kaynaklar

[1] Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing mitre att&ck risk using a cyber-security culture framework. *Sensors*, *21*(9), 3267.

[2] Kwon, R., Ashley, T., Castleberry, J., Mckenzie, P., & Gourisetti, S. N. G. (2020, October). Cyber threat dictionary using mitre att&ck matrix and nist cybersecurity framework mapping. In *2020 Resilience Week (RWS)* (pp. 106-112). IEEE.

[3] Sezer, E. C., Kil, C., & Ning, P. (2010). Automated software vulnerability analysis. *Cyber Situational Awareness: Issues and Research*, 201-223.

[4] Kim, K., Alfouzan, F. A., & Kim, H. (2021). Cyber-attack scoring model based on the offensive cybersecurity framework. *Applied Sciences*, *11*(16), 7738.

[5] Xiong, W., Legrand, E., Åberg, O., & Lagerström, R. (2022). Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. *Software and Systems Modeling*, *21*(1), 157-177.

[6] Bagui, S. S., Mink, D., Bagui, S. C., Ghosh, T., Plenkers, R., McElroy, T., ... & Shabanali, S. (2023). Introducing uwf-zeekdata22: A comprehensive network traffic dataset based on the mitre att&ck framework. *Data*, *8*(1), 18.

[7] Kielland, C. (2023). *Information Security Performance Evaluation: Building a security metrics library and visualization dashboard* (Master's thesis).

[8] Chukwu, C. J. (2023). *Leveraging the MITRE ATT&CK Framework to Enhance Organizations Cyberthreat Detection Procedures* (Doctoral dissertation, Carleton University).

[9] Rajesh, P., Alam, M., Tahernezhadi, M., Monika, A., & Chanakya, G. (2022, September). Analysis of cyber threat detection and emulation using mitre attack framework. In *2022 International Conference on Intelligent Data Science Technologies and Applications (IDSTA)* (pp. 4-12). IEEE.

[10] Strom, B. E., Battaglia, J. A., Kemmerer, M. S., Kupersanin, W., Miller, D. P., Wampler, C., ... & Wolf, R. D. (2017). Finding cyber threats with ATT&CK-based analytics. *The MITRE Corporation, Bedford, MA, Technical Report No. MTR170202*.