



AĞ SALDIRI SİMÜLASYONU: WANNACRY RANSOMWARE ATTACK

NETWORK ATTACK SIMULATION: WANNACRY RANSOMWARE ATTACK

Öğr. Gör. Çisem YAŞAR

İstanbul Gelişim Meslek Yüksekokulu, Bilgisayar Teknolojileri Bölümü, Avcılar, İstanbul.

ORCID NO: 0000-0002-0765-861X

Atakan EREZ

İstanbul Gelişim Meslek Yüksekokulu, Bilgisayar Teknolojileri Bölümü, Avcılar, İstanbul.

ORCID NO: 0009-0003-4266-1763

Murat KAZMA

İstanbul Gelişim Meslek Yüksekokulu, Bilgisayar Teknolojileri Bölümü, Avcılar, İstanbul.

ORCID NO: 0009-0009-8515-292X

ÖZET

Günümüzde bilgi teknolojilerindeki hızlı ilerleme, bireylerin ve kuruluşların dijital dünyadaki varlıklarını koruma ihtiyacını artırmıştır. Siber güvenlik, dijital ortamların güvenliğinin sağlanması açısından kritik bir rol oynamaktadır. Özellikle kötü amaçlı yazılımlar ve fidye yazılımları, siber güvenlik tehditlerinin başında yer almaktadır. Bu çalışmada iki önemli siber güvenlik olayı üzerinde inceleme sağlanmıştır. Bunlar; UnrealIRCd yazılımındaki güvenlik açıkları ve WannaCry fidye yazılımıdır. Ayrıca siber güvenlik alanındaki bir güvenlik açığının nasıl istismar edildiği ve etkileri hakkında bilgi verilmiştir. UnrealIRCd yazılımı, Internet Relay Chat (IRC) üzerinde çalışan popüler bir açık kaynaklı sohbet sunucusudur. Ancak, bu yazılımda keşfedilen güvenlik açıklıkları, siber saldırganlar tarafından istismar edilerek önemli bir siber güvenlik olayının ortaya çıkmasına neden olmuştur. Çalışmada, UnrealIRCd yazılımında tespit edilen güvenlik açıklıkları, açıklıkların detayları ve bu açıklıklardan nasıl yararlanıldığından bahsedilmiştir. WannaCry fidye yazılımı, 2017 yılının Mayıs ayında dünya genelinde büyük bir siber saldırının yaşanmasına sebep olmuştur. WannaCry yazılımı, Microsoft Windows işletim sistemlerindeki EternalBlue isimli güvenlik açığını kullanarak hızla yayılım göstermiş ve sistemlerdeki dosyaları şifreleyerek kullanıcıların erişimini engellemiştir. Fidye talep eden WannaCry yazılımı, özellikle sağlık hizmetleri ve kritik altyapıların hedef alınmasıyla dikkat çekmesinin yanında büyük ekonomik zararlara da yol açmıştır. Bu bağlamda çalışmada WannaCry fidye yazılımı saldırısı için bir senaryo oluşturulmuş ve Cisco Packet Tracer simülasyon yazılımında senaryonun benzetimi gerçekleştirilmiştir. Bu benzetim, bir saldırının nasıl gerçekleştiği ve etkilerini inceleme fırsatı sunulmasına yardımcı olmuştur. Yapılan çalışmanın amacı, kurumsal güvenliği artırmak için olası güvenlik açıklarının tespitini sağlamak ve bu açıklıkların nasıl istismar edilebileceğini göstermektir. Aynı zamanda Nessus programı ile gerçekleştirilen güvenlik taramaları sonucunda, çeşitli güvenlik açıklıkları ve zayıf noktalarının belirlenmesine yardımcı olmaktadır. Çalışma kapsamında gerçekleştirilen simülasyon sonucunda bir sistemde bulunan güvenlik açıklıkları ve zayıf noktaların kurumsal güvenlik politikalarını güçlendirmeye yönelik önemli katkılar sağladığı görülmüştür. Kurumların, sistemlerini düzenli olarak taramaları, güncel tutmaları ve güvenlik politikalarını sürekli olarak gözden geçirmeleri önerilmektedir. Ayrıca, kurum çalışanlarının siber güvenlik



konusunda farkındalık oluşturmaları için bu konuda bilinçlendirilmesi ve eğitimlerin artırılması gerekliliğine vurgu yapılmıştır.

Anahtar Kelimeler: Siber güvenlik, UnrealIRCd, WannaCry, EternalBlue, Nessus, Cisco Packet Tracer

ABSTRACT

Today, the rapid advancement in information technologies has increased the need for individuals and organizations to protect their assets in the digital world. Cyber security plays a critical role in ensuring the security of digital environments. In particular, malware and ransomware are at the forefront of cyber security threats. In this study, two important cyber security incidents are examined. These are; vulnerabilities in UnrealIRCd software and WannaCry ransomware. In addition, information about how a vulnerability in the field of cyber security is exploited and its effects are given. UnrealIRCd software is a popular open source chat server running on Internet Relay Chat (IRC). However, vulnerabilities discovered in this software have been exploited by cyber attackers, resulting in a significant cybersecurity incident. In this study, the vulnerabilities detected in the UnrealIRCd software, the details of the vulnerabilities and how these vulnerabilities are exploited are mentioned. WannaCry ransomware caused a major cyber attack worldwide in May 2017. The WannaCry software spread rapidly using the vulnerability named EternalBlue in Microsoft Windows operating systems and encrypted files in the systems and prevented users from accessing them. WannaCry software, which demands ransom, has caused great economic damage as well as attracting attention especially by targeting health services and critical infrastructures. In this context, a scenario for the WannaCry ransomware attack was created and simulated in Cisco Packet Tracer simulation software. This simulation helped to provide an opportunity to examine how an attack occurs and its effects. The aim of the study is to identify potential vulnerabilities and show how these vulnerabilities can be exploited to improve organizational security. At the same time, it helps to identify various security vulnerabilities and weak points as a result of security scans performed with the Nessus program. As a result of the simulation carried out within the scope of the study, it was seen that the vulnerabilities and weak points in a system make significant contributions to strengthening corporate security policies. It is recommended that organizations regularly scan their systems, keep them up to date and constantly review their security policies. In addition, it was emphasized that the employees of the organization should be made aware of cyber security and trainings should be increased.

Keywords: Cybersecurity, UnrealIRCd, WannaCry, EternalBlue, Nessus, Cisco Packet Tracer

GİRİŞ

Malware kavramı “Kötü Amaçlı Yazılım” anlamına gelen “Malicious Software” kelimelerinin kısaltmasından oluşmaktadır. Malware, bilgisayar ve akıllı telefon gibi teknolojik cihazlara yönelik zarar vermek amacıyla tasarlanmış yazılım olarak tanımlanmaktadır. Verebileceği zararlar arasında cihazların işlevini bozmak, hassas bilgilere erişmek, yetkisiz erişim sağlamak yer almaktadır (Kabakuş, Doğru ve Çetin, 2015). Kötü amaçlı yazılımlar farklı türlerde olabilir; truva atı, solucan, keylogger ya da fidye yazılımları örnek verilebilir. Bu tür kötü amaçlı yazılımlar siber güvenlik olaylarının yaşanmasına sebep olmaktadır. 2010 yılında Internet Relay Chat (IRC) protokolü üzerinde çalışan popüler açık kaynaklı sohbet sunucu olan

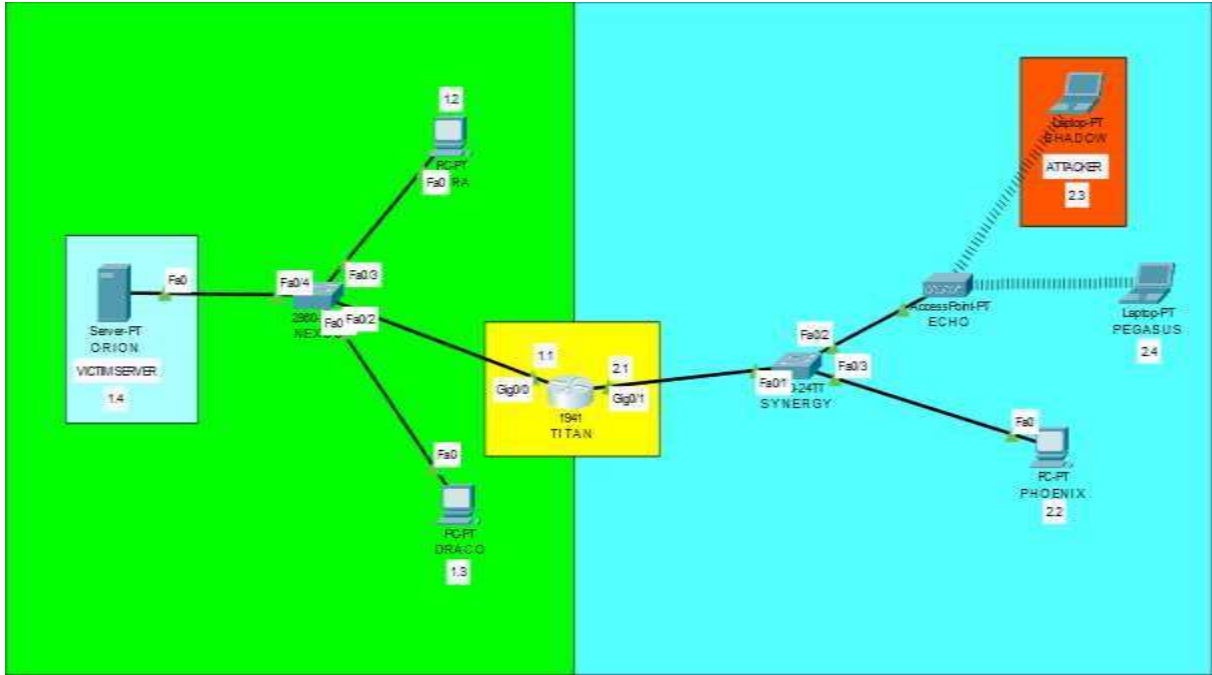


UnrealIRCD üzerinde güvenlik açığı tespit edildi. Bu yazılımda bulunan güvenlik açığı kötü niyetli kişiler tarafından istismar edilmiş ve siber güvenlik olayının yaşanmasına neden olmuştur (Hsu ve Lee, 2011). Windows işletim sisteminin Sunucu İleti Bloğu (SMB)

protokülünde bulunan EternalBlue adlı istismar sadece bir paket gönderimi sağlayarak cihazda uzaktan kod çalıştırılmasını gerçekleştirir. Bu durumda bir siber güvenlik olayının yaşanmasına neden olmaktadır (Liu vd., 2022). EternalBlue istismarı, 2017 yılında WannaCry ve NotPetya gibi büyük yankı uyandıran saldırıların oluşumuna neden olmuştur (Alain vd., 2024). WannaCry bir tür fidye yazılımı olarak bilinmektedir. Fidye yazılımları veya diğer bir adıyla bilinen ransomware saldırılarıdır. Bu tür saldırılar bilgisayar sistemlerine bulaşarak kullanıcıların dosyalarını şifreleyen ve şifrelenmiş dosyaların çözülmesi veya tekrardan erişime açılması için fidye talep eden kötü niyetli yazılımlar olarak bilinmektedir (Begovic vd., 2023). Günümüzde siber suçlar küresel çapta büyüme göstermektedir. Fidye yazılımları ise saldırı türleri arasında öne çıkan ve büyük bir tehdit oluşturan tür olarak dikkat çekmektedir (Singleton vd., 2021). Fidye yazılımları, bulaştıkları sistemde bulunan dosyaları şifreleyerek kullanıcının erişimini engellemekte ve kullanıcının şifreyi bilmemesi durumunda kullanılamaz hale gelmesine neden olmaktadır. Siber saldırgan mağdur olan kullanıcının dosyalara erişimini sağlayabilmek için kullanıcıdan fidye talep etmektedir. Genellikle talep edilen fidye kripto para ile ödenmesi istenmektedir. Kripto paranın tercih edilme sebebi ise siber saldırganın kimliğinin açığa çıkma olasılığının düşük olmasıdır. Ödenilen fidye miktarına rağmen bazı durumlarda siber saldırganlar dosyaların açılıp açılmama durumuna kesinlikle garanti vermezler (Erdoğan, 2024). 2017 yılında birçok ülkede Windows işletim sistemi kullanan bilgisayarları hedef olarak gerçekleştirilen saldırı WannaCry fidye yazılımı olarak bilinmektedir. WannaCry fidye yazılımı özellikle İngiltere NHS (National Health Service)'ye yapılan saldırıda hastane ve doktorları hedef olarak hastaların geri çevrilmesiyle sağlık hizmetinin verilemeyecek duruma gelmesi sonucunda sağlık sisteminde aksaklıkların yaşanmasına neden olmuştur. Aynı zamanda Rusya'da İçişleri Bakanlığı sistemlerinin etkilenmesi ve pek çok ülkede on binlerce kişi ve kurumu da etkileyerek milyonlarca dolar hasara neden olmuştur (Kılıç, 2019; Şimşek ve Güler, 2021). Literatüre bakıldığında ise; Maurya vd. (2018) yaptıkları çalışmada, fidye yazılımlarının gelişimi ve popüler olan fidye yazılımlarının genel özelliklerini incelemişlerdir. Farklı fidye yazılımlarının ortaya çıkardığı sorunu örneklemek amacıyla birkaç fidye yazılımı saldırısı vaka çalışması gerçekleştirmişlerdir. Fernando, Komninos ve Chen (2020) yaptıkları çalışmada, makine öğrenmesi ve derin öğrenme algoritmalarını kullanarak fidye yazılımlarının tespitine yönelik araştırma yapmışlardır. Guvçi ve Şenol (2023) yaptıkları çalışmada, fidye yazılımı saldırılarının kurumlar ve bireyler üzerindeki etkisini analiz etme, mevcut önlem ve etkisini azaltma stratejilerini değerlendirmişlerdir. Bu çalışmada ise WannaCry fidye yazılımı saldırısı için bir senaryo oluşturulmuş ve Cisco Packet Tracer simülasyon yazılımında senaryonun benzetimi gerçekleştirilmiştir. Bu benzetim, bir saldırının nasıl gerçekleştiği ve etkilerini inceleme fırsatı sunulmasına yardımcı olmuştur.

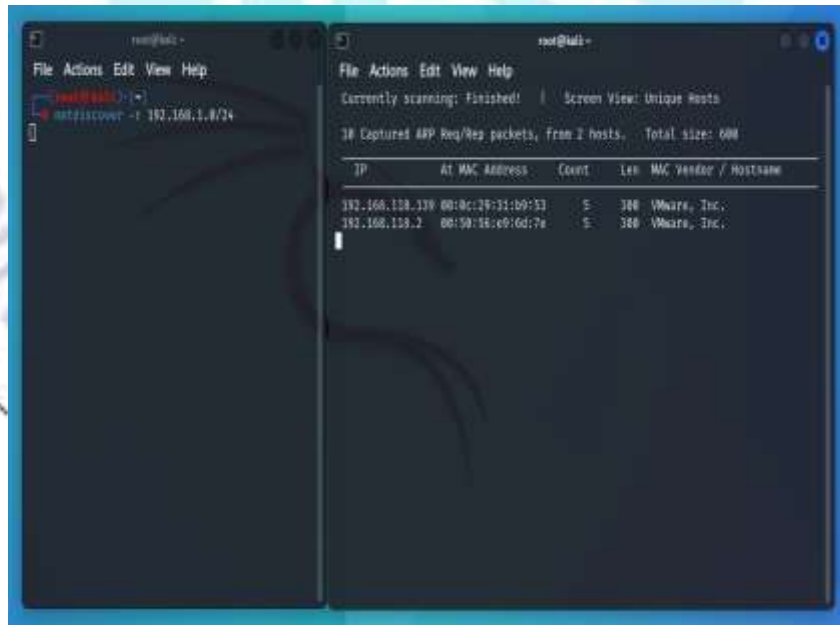
ARAŞTIRMA VE BULGULAR

Çalışma kapsamında oluşturulan senaryo; etik hacker Alex (kod adı Shadow) tarafından gerçekleştirilmiştir. EternalBlue zafiyetini kullanarak WannaCry fidye yazılımını hedef sisteme yüklemesi ile sonuçlandırılmıştır. Tasarlanan senaryo ağ yapısı Şekil 1.1'de gösterilmektedir.



Şekil 1.1. Tasarlanan senaryo ağ yapısı

Öncelikle, Netdiscover aracılığı ile ağa bağlı olan cihazların IP adresi aralığı taraması sağlanmıştır. Şekil 1.2’de hedef işletim sisteminin IP adresinin tespit edildiği görülmektedir.



Şekil 1.2. Netdiscover ile IP adresi tespiti

Bağlantı kurulduktan sonra ağ üzerindeki IP adreslerini ve cihazları tespit etmek için Nmap aracılığıyla port taraması gerçekleştirilmiştir. Şekil 1.3’de görülen Nmap taraması sonucunda

cihazın Windows işletim sistemine sahip olduğu ve 445 numaralı SMB portunun açık olduğu tespit edilmiştir.



```
root@kali: ~  
root@kali:~# nmap 192.168.118.139  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-14 06:13:01 EDT  
Nmap scan report for 192.168.118.139  
Host is up (0.0020s latency).  
Not shown: 999 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
445/tcp   open  microsoft-ds  
MAC Address: 08:00:27:31:B9:53 (VMware)  
Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds  
root@kali:~#
```

Şekil 1.3. Nmap aracı ile IP adresi taraması

Tarama sonucunda cihazın SMB servisi versiyon 1.0'ı çalıştırdığı ve Şekil 1.4'de görülen SMB versiyonunun CVE-2017-0143 olarak bilinen bir zafiyete sahip olduğu tespit edilmiştir.



```
root@kali: ~  
root@kali:~# nmap --script vuln -p 445 192.168.118.139  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-14 06:58:07 EDT  
Nmap scan report for 192.168.118.139  
Host is up (0.0013s latency).  
Not shown: 999 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
445/tcp   open  microsoft-ds  
MAC Address: 08:00:27:31:B9:53 (VMware)  
  
Host script results:  
_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED  
_smb-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED  
_smb-vuln-ms17-010:  
  VULNERABLE:  
  Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)  
  State: VULNERABLE  
  IDs: CVE:CVE-2017-0143  
  Risk factor: HIGH  
  A critical remote code execution vulnerability exists in Microsoft SMBv1  
  servers (ms17-010).  
  
Disclosure date: 2017-03-14  
References:  
  https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-atta  
cks/  
  https://technet.microsoft.com/en-us/library/security/ms17-010.aspx  
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143  
_smb-vuln-ms10-054: false  
  
Nmap done: 2 IP addresses (1 host up) scanned in 32.39 seconds  
root@kali:~#
```

Şekil 1.4. Nmap ile tarama sonucu hizmetlerin listelenmesi

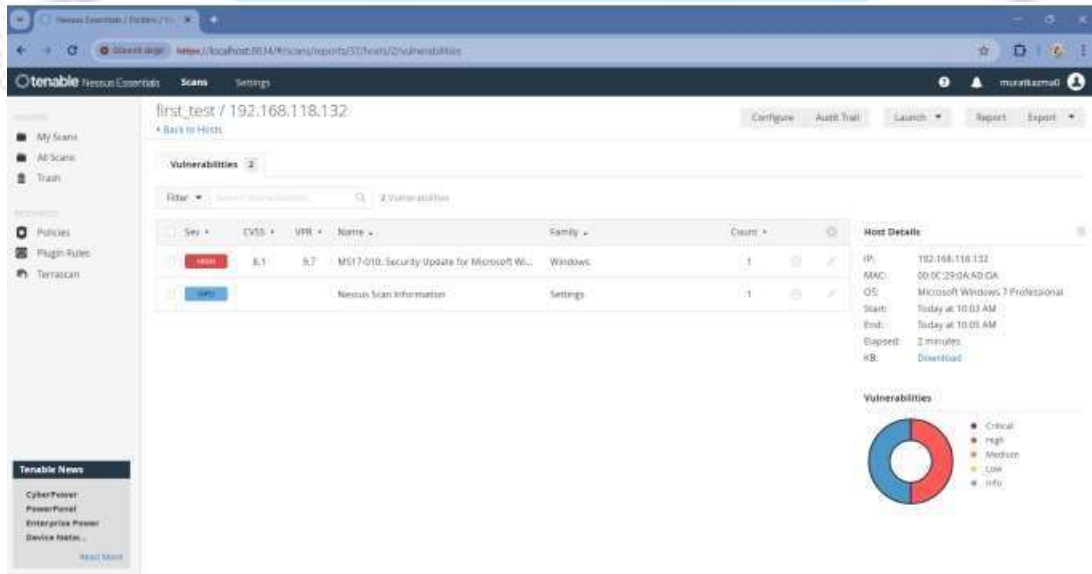
SMB versiyonunda tespit edilen olası zafiyetler değerlendirilmiş ve bu zafiyetlerden faydalanmak amacıyla Metasploit Framework’ü kullanılmıştır. Metasploit Framework’ünde bulunan “*exploit*” komutu ile sömürü modülü çalıştırılmış ve MS17-010 zafiyetini kullanarak hedef sistemde uzaktan kod yürütme (RCE) saldırısı gerçekleştirilmiştir. Aynı zamanda “*meterpreter*” saldırgan hedef sistemlere sızmak ve erişmek için kullanılmıştır. Şekil 1.5’de hedef sisteme erişim sağlanmış ve WannCry fidye yazılımı aktif hale getirilmiştir.

```
meterpreter >
meterpreter > pwd
C:\Windows
meterpreter > upload /root/Desktop/WannaCry.EXE C:/Windows/WannaCry.exe
[*] Uploading : /root/Desktop/WannaCry.EXE → C:/Windows/WannaCry.exe
[*] Uploaded 3.35 MiB of 3.35 MiB (100.0%): /root/Desktop/WannaCry.EXE → C:/Windows/WannaCry.exe
[*] Completed : /root/Desktop/WannaCry.EXE → C:/Windows/WannaCry.exe
meterpreter > shell
Process 2576 created.
Channel 3 created.
Microsoft Windows [S*rm 6.1.7601]
Telif Hakk* (c) 2009 Microsoft Corporation. T*m haklar* saklıdır.

C:\Windows>WannaCry.exe
WannaCry.exe
C:\Windows>
```

Şekil 1.5. Hedef sisteme erişim sağlama

Hedef sisteme WannCry fidye yazılımının yüklenmesi sonucunda Nessus Essentials aracılığıyla sistemde güvenlik taraması gerçekleştirilmiştir. Şekil 1.6’da gösterilen tarama sonucunda, sistemde kritik önem taşıyan güvenlik açığı olduğunu göstermektedir. Bu güvenlik açığı, saldırganların sistemi ele geçirmesine ve kontrol altına almasına neden olabilir. Bu nedenle, bu güvenlik açığının en kısa sürede giderilmesi önerilmektedir.



Şekil 1.6. Nessus Essentials ile tarama sonucu

Oluşturulan senaryonun sonucunda elde edilen bulgular;

- **SMB Zafiyeti:** Ağ üzerinden dosya paylaşımını sağlayan SMB protokolündeki güvenlik zafiyetidir ve saldırganların uzaktan sistemlere erişip zarar vermesine olanak tanımaktadır. Bu tür açıklıklar, genellikle yazılım güncellemeleri ve yamalarla kapatılabilir.
- **MS17-010 Zafiyeti:** SMB protokolünde bulunan güvenlik açıklıklarından kaynaklanmaktadır ve bu açıklıklar WannaCry fidye yazılımı gibi zararlı saldırıları gerçekleştirmek için kullanılabilir.
- **Ağ Güvenliği Zayıflıkları:** Ağ topolojisinde, özellikle ağın bölünmesi ve cihazların farklı güvenlik özelliklerine sahip olması nedeniyle çeşitli güvenlik zayıflıkları belirlenmiştir. Bu zayıflıklar, saldırganların çeşitli saldırı türlerini kullanarak ağa sızmasına imkan tanımaktadır.
- **Güncellenmemiş Sistemler:** Güvenlik yamalarının uygulanmadığı sistemlerde WannaCry gibi fidye yazılımlarına karşı savunmasız oldukları tespit edilmiştir.
- **Fidye Yazılımının Yayılma Potansiyeli:** Oluşturulan simülasyon sırasında, WannaCry fidye yazılımının ağ üzerindeki diğer sistemlere hızla yayılabildiği ve önemli veri kayıplarına yol açabileceği tespit edilmiştir.
- **Küresel Bir Siber Tehdit ve Ağ Solucanı:** WannaCry, 12 Mayıs 2017'de başlayan ve dünya genelinde büyük bir yankı uyandıran bir kripto fidye yazılımı saldırısıdır. Bu yazılım, kullanıcıların dosyalarını şifreleyerek erişimlerini engeller ve dosyaların şifresini çözmek için belirli bir fidye talep eder. WannaCry'nin en dikkat çeken özelliklerinden biri ise Microsoft Windows işletim sistemlerindeki EternalBlue adlı güvenlik açığını kullanarak kendini yayabilme yeteneğidir. Bu özellik, fidye yazılımının bir ağ solucanı olarak da tanımlanmasını sağlamaktadır.
- **Fidye Talebi ve Küresel Etkisi:** WannaCry, kurbanlarının sistemlerini ele geçirip dosyalarını şifreler ve fidye talep etmektedir. Aynı zamanda fidye talebi karşılanmazsa dosyaların tamamen silineceği tehdidini de içermektedir. WannaCry saldırısı özellikle sağlık, finans ve kritik altyapı hizmetlerini hedef almış ve dünya genelinde 150'den fazla ülkede ve 200.000'den fazla bilgisayar sistemini etkilemektedir.
- **WannaCry Fidye Yazılımından Kurtulma Yöntemleri:** Bilgisayarınızı yeniden başlatarak “Güvenli Mod” ya da “Ağ Bağlantılı Güvenli Mod” seçeneğini kullanarak WannaCry fidye yazılımı silinmesi önerilir. Başka bir yöntem ise saatlik ya da günlük yedekleme stratejileri ile bu tür saldırılardan etkilenmeden verilerinizi geri yükleyebilir ve fidye ödemekten kaçınabilirsiniz.

SONUÇ VE ÖNERİLER

Bu çalışmada WannaCry fidye yazılımı saldırısı için bir senaryo oluşturulmuş ve Cisco Packet Tracer simülasyon yazılımında senaryonun benzetimi gerçekleştirilmiştir. Oluşturulan senaryoda hedef sistemin IP adresi tespit edilmiş ve IP adresi üzerinde port taraması yapılmıştır. Tarama sonucunda açık port ve MS17-010 zafiyeti bulunmuştur. İlgili zafiyetten yararlanmak için Metasploit Framework'ü kullanılmıştır. Meterpreter yardımı ile de hedef sisteme giriş sağlanmış ve WannaCry fidye yazılımı aktif edilmiştir. Aynı zamanda hedef sistemde Nessus Essentials programı ile gerçekleştirilen güvenlik taramaları sonucunda, çeşitli güvenlik açıklıkları ve zayıf noktaları belirlenmiştir. Sonuç olarak, bir sistemde bulunan güvenlik açıklıkları ve zayıf noktaların tespiti sağlanmıştır. Bu bağlamda, kurumların, sistemlerini düzenli olarak taramaları, güncel tutmaları ve güvenlik politikalarını sürekli olarak gözden



geçirmeleri önerilmektedir. Ayrıca, kurum çalışanlarının siber güvenlik konusunda farkındalık oluşturma için bu konuda bilinçlendirilmesi ve eğitimlerin artırılması önerilmektedir.

KAYNAKÇA

Alain, P., Autrel, F., Bouabdallah, A., François, J., & Doyen, G. (2024, June). How Fast Does Malware Leveraging EternalBlue Propagate? The case of WannaCry and NotPetya. In *2024 IEEE 10th International Conference on Network Softwarization (NetSoft)* (pp. 399-404). IEEE.

Begovic, K., Al-Ali, A., & Malluhi, Q. (2023). Cryptographic ransomware encryption detection: Survey. *Computers & Security*, 132, 103349.

Erdoğan, M. (2024). Siber suçlarla ilgili 2000-2023 yılları arasındaki çalışmaların bibliyometrik analizi (*Master's thesis, Hitit Üniversitesi*).

Fernando, D. W., Komninos, N., & Chen, T. (2020). A study on the evolution of ransomware detection using machine learning and deep learning techniques. *IoT*, 1(2), 551-604.

Guvci, F., & Senol, A. (2023). An improved protection approach for protecting from ransomware attacks. *Journal of Data Applications*, 1, 69-82.

Hsu, Y., & Lee, D. (2011). Machine learning for implanted malicious code detection with incompletely specified system implementations. In *2011 19th IEEE International Conference on Network Protocols* (pp. 31-36). IEEE.

Kabakuş, A. T., Doğru, İ. A., & Çetin, A. (2015). Android kötücül yazılım tespit ve koruma sistemleri. *Erciyes Üniversitesi Fen Bilimleri Enstitüsü Fen Bilimleri Dergisi*, 31(1), 9-16.

Kılıç, Ç. (2019). Düünden bugüne fidye yazılımların (Ransomware) gelişimi ve geleceği (*Master's thesis, Lisansüstü Programlar Enstitüsü*).

Liu, Z., Chen, C., Zhang, L. Y., & Gao, S. (2022). Working mechanism of eternalblue and its application in ransomworm. In *International Symposium on Cyberspace Safety and Security* (pp. 178-191). Cham: Springer International Publishing.

Singleton, C., DeBeck, C., Chung, J., McMillen, D., Craig, S., & Moore, S. (2021). X-Force Threat Intelligence Index 2021. *IBM Security*, 43-5.

Şimşek, B. Ş., & Güler, İ. (2021). Lisanssız Yazılım Kullanımı ve Farkındalık. In *2021 5th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)* (pp. 243-245). IEEE.

Maurya, A. K., Kumar, N., Agrawal, A., & Khan, R. A. (2018). Ransomware: evolution, target and safety measures. *International Journal of Computer Sciences and Engineering*, 6(1), 80-85.