Araştırma *Yavuz&Tuna/Kırklareli University Journal of Engineering and Science 5-2(2019) 200-209*
DOI: 10.34186/klujes.578590 *Geliş Tarihi:06.11.2019 Kabul Tarihi: 31.12.2019*

BİLGİ GÜVENLİĞİ TEHDİTLERİ: YAZILIM TANIMLI AĞLAR GELENEKSEL BİLGİSAYAR AĞLARINA KARŞI

Abdullah Yavuz, Gürkan Tuna[1*]

[1] Trakya Üniversitesi, Edirne Teknik Bilimler MYO, Edirne.

ÖZET

Yazılım tanımlı ağlar bakım, maliyet ve yönetim kolaylığı açılarından avantajlara sahiptir. Öte yandan, geleneksel bilgisayar ağları uzun yıllardır bilgi güvenliği tehditleri açısından sınanmış olmakla birlikte gerçek saha uygulamalarında yazılım tanımlı ağlar üzerinde yapılan çalışmalar nispeten azdır. Yazılım tanımlı ağların bilgi güvenliği tehditleri açısından ele alınmasının özellikle ağ yöneticileri için kritik önem taşıdığı dikkate alınarak, bu çalışmada yazılım tanımlı ağlar ile geleneksel bilgisayar ağlarının bilgi güvenliği tehditlerine karşı zafiyetleri değerlendirilmiş ve çözüm önerileri sunulmuştur. Gerçekleştirilen benzetim çalışmalarında IP Spoofing, SYN Flood, RST/FIN Flood, SYN-ACK Flood, UDP Flood, ARP Poisoning ve Distributed Denial of Service saldırıları gerçekleştirilmiştir. Gerçekleştirilen benzetim çalışmalarının sonuçları, geleneksel bilgisayar ağlarına kıyasla ARP Poisoning saldırısı dışında yazılım tanımlı ağların daha fazla güvenlik zafiyeti taşıdığı görülmektedir. Ancak alınacak bazı tedbirler ile potansiyel birçok bilgi güvenliği saldırısının etkileri ortadan kaldırılabilir veya azaltılabilir.

Anahtar Kelimeler: Yazılım Tanımlı Ağlar, Geleneksel Bilgisayar Ağları, Tehditler, Güvenlik.

ABSTRACT

Software-defined networks have advantages in terms of maintenance, cost and ease of management. On the other hand, traditional computer networks have been tested for information security threats for many years, but in real-field applications, studies on software-defined networks are relatively small. Considering that software-defined networks are of critical importance for network administrators, in this study, vulnerabilities of software-defined networks against information security threats were evaluated and solutions were proposed. In the simulation studies, IP Spoofing, SYN Flood, RST / FIN Flood, SYN-ACK Flood, UDP Flood, ARP Poisoning and Distributed Denial of Service attacks were carried out. The results of the simulation studies show that except for ARP Poisioning, software defined networks carry more security vulnerability compared to traditional computer networks. However, with some measures, the effects of many potential information security attacks can be eliminated or mitigated.

Keywords: Software Defined Networks, Traditional Computer Networks, Threats, Security.

*gurkantuna@trakya.edu.tr, https://orcid.org/0000-0002-6466-4696

DOI: 10.34186/klujes.578590 *Geliş Tarihi:06.11.2019 Kabul Tarihi: 31.12.2019*

1. GİRİŞ

Geleneksel bilgisayar ağ mimarisi merkeziyetçi ve karmaşık olduğundan bu mimariye dayalı ağlarda kısıtlı esneklik ve sorun giderme zorlukları bulunmaktadır. Bu mimariye dayalı ağlar üreticiye bağlıdır ve ağ yapılandırmasında herhangi bir değişiklik yapmak oldukça zor ve maliyetlidir [1]. Geleneksel bilgisayar ağ altyapılarının kısıtlamalarını ortadan kaldırabilmek için yazılım tanımlı ağlar önerilmiştir. Yazılım tanımlı ağlarda geleneksel bilgisayar ağ mimarisinin altyapısında bir bütün olarak bulunan veri ve kontrol düzlemleri ayrılmaktadır [2]. Böylece, ağ ve yönetim sistemlerinin basitleştirilmesi ve otonom bir yapıya kavuşması hedeflenmektedir [2]. Mevcut donanım altyapısını kullanarak sanal ağlar oluşturmak ve onu kısa sürede ve düşük maliyetle esnek bir ağ olarak tanımlayabilmek için programlama kilit noktadır [3,4]. Bu nedenle yazılım tanımlı ağların tarihsel gelişimine bakıldığında programlanabilir ağlar üzerine kurulu olduğu görülebilir. 1990'lı yıllarda ortaya atılmış olan programlanabilir ağlar üreticilerin kurallarına bağlı kalınmasını zorunlu kılmakta ve üreticilerin müsaade ettiği derecede açıktı. Farklı üretici cihazlarında aynı yapılandırmanın sağlanamaması nedeniyle kısıtlı başarıya ulaşmışlardır [5]. Aktif ağlar [6], Programlanabilir ATM ağları [7], Network Control Point (NCP) [8] ve Routing Control Platform (RCP) [9] en bilinen örnekler arasındadır.

Geleneksel bilgisayar ağlarından farklı olarak etkin bir ağ yapılandırması sağlayan ve programlanabilir ağ yönetimi yaklaşımı sunan yazılım tanımlı ağların tarihsel gelişimi incelenirse yazılım tanımlı ağ teriminin OpenFlow çalışmalarının ardından ortaya çıktığı görülebilir [10]. OpenFlow ağ anahtarlayıcı ve yönlendiricilerin ağ üzerinden yönlendirme düzlemine erişim sağlayan bir iletişim protokolüdür [10]. OpenFlow ağları daha dinamik, yönetilebilir, düşük maliyetli ve uygulanabilir hale getirerek hem fiziksel hem de sanal ağ anahtarlayıcı ve yönlendirici gibi ağ donanımlarının doğrudan programlanmasını sağlar [11]. OpenFlow üzerine çalışmalar yapmak amacıyla kurulan Open Networking Foundation (ONF) [12] yazılım tanımlı ağ mimarisi için altyapı katmanı, kontrol katmanı ve uygulama katmanından oluşan 3 katmanlı bir mimari önermiştir [13]. Bu katmanlar arasındaki iletişimi sağlamak için ise kuzey ve güney ara yüzü önerilmiştir.

DOI: 10.34186/klujes.578590 *Geliş Tarihi:06.11.2019 Kabul Tarihi: 31.12.2019*

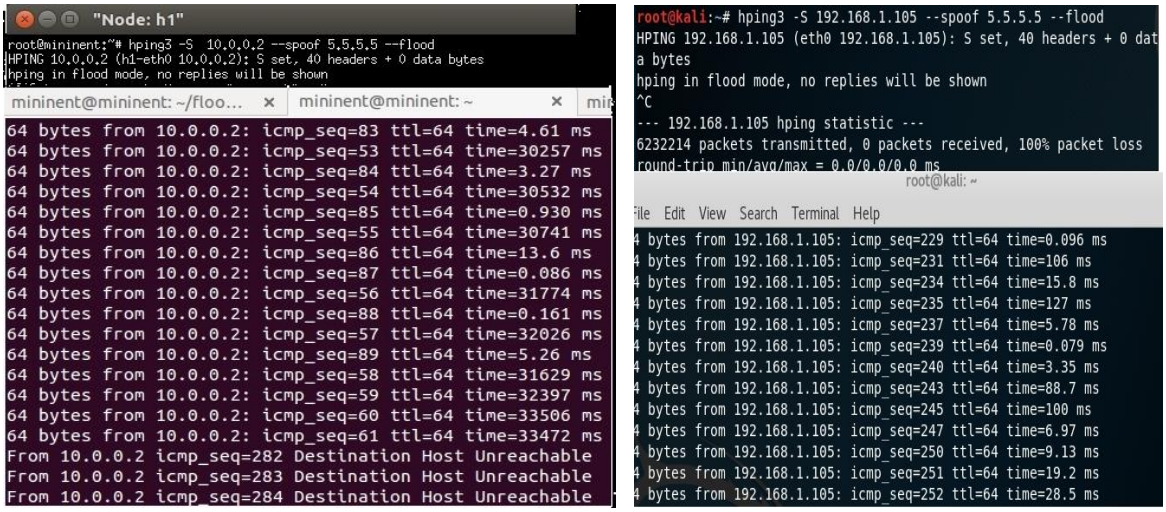
Günümüzde internet kullanımının yaygınlaşması nedeniyle ağ güvenliğini sağlamak kaçınılmaz bir gereklilik haline gelmiştir. Ağ güvenliği, bir bilgisayar ağının ve ağ tarafından erişilebilen kaynakların yetkisiz erişimi, kötüye kullanımı, değiştirilmesi veya reddedilmesini önlemek ve izlemek için kabul edilen politika ve uygulamalardan oluşmaktadır. Ağ güvenliği, ağ yöneticisi tarafından kontrol edilen bir ağdaki verilere erişim yetkisini içerir. İşletim sistemleri ve kullanılan yazılımlar daha işlevsel ve kapsamlı hale geldikçe olası tehditler de artar. Ağ güvenliği sorunluysa verilere erişme hakları olmayan davetsiz misafirler, ağ kullanıcılarına ait değerli ve özel bilgilere erişebilir [14]. Geleneksel bilgisayar ağları üzerinden iletişim kuran bilgisayar sistemlerini korumak olarak adlandırılabilecek olan siber güvenliğin amacı bilgi güvenliği risklerini sınırlamak ve bilişim teknolojilerini kötü niyetli saldırganlardan korumaktır. Verilerin gizliliğini, bütünlüğünü ve erişilebilirliğini korumayı amaçlar. Geleneksel bilgisayar ağları bilgi güvenliği tehditlerine karşı uzun yıllardır denenmiştir. Öte yandan, yazılım tanımlı ağlar üzerinde sınırlı sayıda bilgi güvenliği değerlendirmesi yapılmıştır. Bu çalışmada, yazılım tanımlı ağların geleneksel bilgisayar ağlarına kıyasla bilgi güvenliği tehditlerine karşı zafiyetleri değerlendirilmiş ve çözüm önerileri ortaya konmuştur. Gerçekleştirilen benzetim çalışmalarında kullanılan saldırı çeşitleri arasında IP Spoofing, SYN Flood, RST/FIN Flood, SYN-ACK Flood, UDP Flood, ARP Poisoning ve Distributed Denial of Service (DDoS) bulunmaktadır.

2. MATERYAL VE METOD

Yazılım tanımlı ağ kontrolcüleri, yazılım tanımlı ağ mimarisinde kontrol katmanında yer almaktadır. Kontrolcü, yazılım tanımlı bir ağın çekirdeğidir. Ağın bir ucundaki ağ cihazları ve diğer ucundaki uygulamalar arasında bulunmakta olup, gelişmiş ağ yönetimi ve uygulama performansı için akış kontrolünü yönetmektedir [15]. Güncel olarak kullanılan yazılım tanımlı ağ kontrolcüleri, OpenFlow protokolüne dayanmaktadır [10]. Yazılım tanımlı ağ kontrolcüleri ağ trafiğini bir ağ operatörünün uyguladığı yönlendirme politikalarına göre doğrudan yönlendirmekte ve böylece bireysel ağ cihazları için otomatik olmayan yapılandırma işlemlerini en aza indirmektedir. Bu çalışma kapsamında gerçekleştirilen benzetim çalışmalarında Hping3 [16] ve Dsniff [17] uygulamaları kullanılmıştır. Yazılım tanımlı ağları oluşturmak için yazılım tanımlı ağ kontrolcüsü olarak Floodlight kontrolcüsü [18] seçilmiş ve

Mininet emülatörü [19] kullanılmıştır. Mininet, bir sanal host, switch, kontrolcü ve bağlantı ağı oluşturan bir ağ emülatörüdür. Oldukça esnek ve özel yönlendirmeye sahip yazılım tanımlı ağlar oluşturmak için OpenFlow'u desteklemektedir. Mininet, araştırma, geliştirme, öğrenme, prototip oluşturma, test etme, hata ayıklama da dahil birçok işlevi desteklemektedir [19]. Çalışma kapsamındaki saldırıları gerçekleştirmek için geleneksel bilgisayar ağlarında Kali Linux [20] sanal makinesi, yazılım tanımlı ağlarda ise oluşturulmuş olan yazılım tanımlı ağ içindeki h1 düğümü kullanılmıştır. Saldırıların hedefi olarak geleneksel bilgisayar ağlarında ana makine, yazılım tanımlı ağda ise h2 düğümü seçilmiştir. Benzetim çalışmasında IP Spoofing, SYN Flood, RST/FIN Flood, SYN-ACK Flood, UDP Flood, DDoS ve ARP Poisoning saldırıları kullanılmıştır.

Şekil 1'de gösterildiği gibi IP Spoofing saldırısı yazılım tanımlı ağda başladıktan kısa bir süre sonra saldırıya maruz kalan h2 düğümü ağdan kopmuş fakat sonra tekrar bağlanmıştır. Ancak daha sonra ağdan tamamen kopmuştur. Öte yandan, geleneksel bilgisayar ağlarında ise saldırıya maruz kalan makine ise ağdan kopmamış fakat kontrol amacıyla gönderilen ping paketlerinde kayıplar olmuştur.



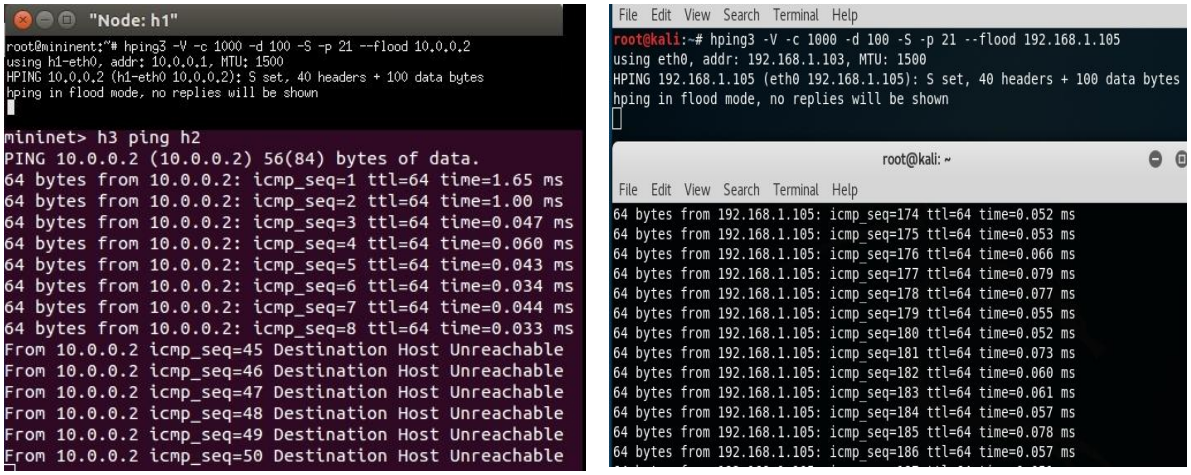
(a) yazılım tanımlı ağ (b) geleneksel bilgisayar ağı

Şekil 1. Saldırı 1 – IP Spoofing.

Şekil 2'de gösterildiği gibi SYN Flood saldırısı yazılım tanımlı ağda başladıktan sonra saldırıya maruz kalan düğüm, ağda kalma süresi değişse bile her denemede ağdan kopmuştur. Geleneksel

DOI: 10.34186/klujes.578590 *Geliş Tarihi:06.11.2019 Kabul Tarihi: 31.12.2019*

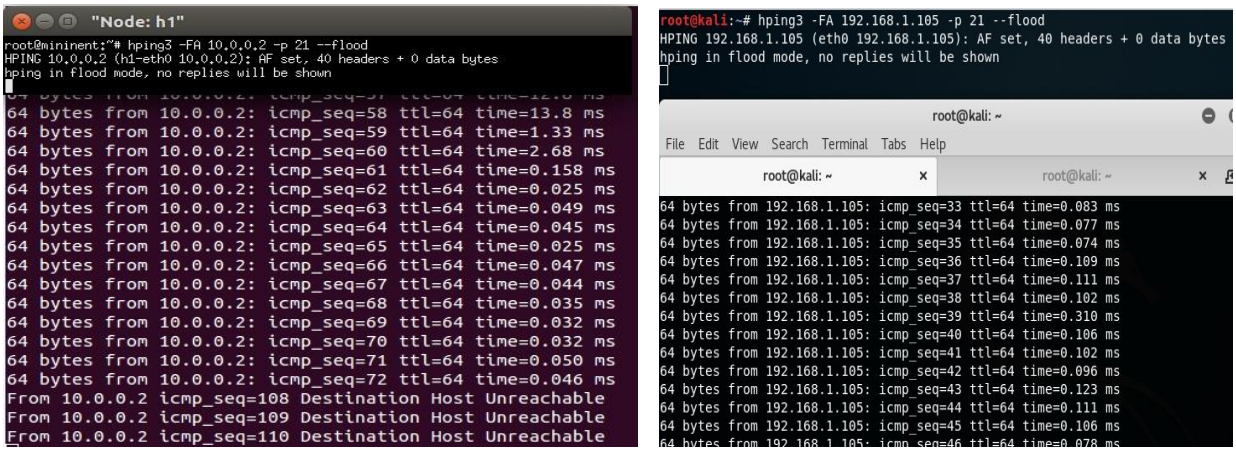
bilgisayar ağlarında saldırıya maruz kalan makine ise saldırıdan etkilenmemiştir.



(a) yazılım tanımlı ağ (b) geleneksel bilgisayar ağı

Şekil 2. Saldırı 2 – SYN Flood.

Şekil 3'te gösterildiği gibi RST/FIN Flood saldırısı yazılım tanımlı ağda başladıktan sonra saldırıya maruz kalan düğüm ağdan kopmuştur. Ağdan tamamen kopmadan önce birkaç defa ağa tekrar bağlanmış olsa bile sonuç değişmemiştir. Geleneksel bilgisayar ağlarında ise saldırıya maruz kalan makine saldırıdan etkilenmemiştir.

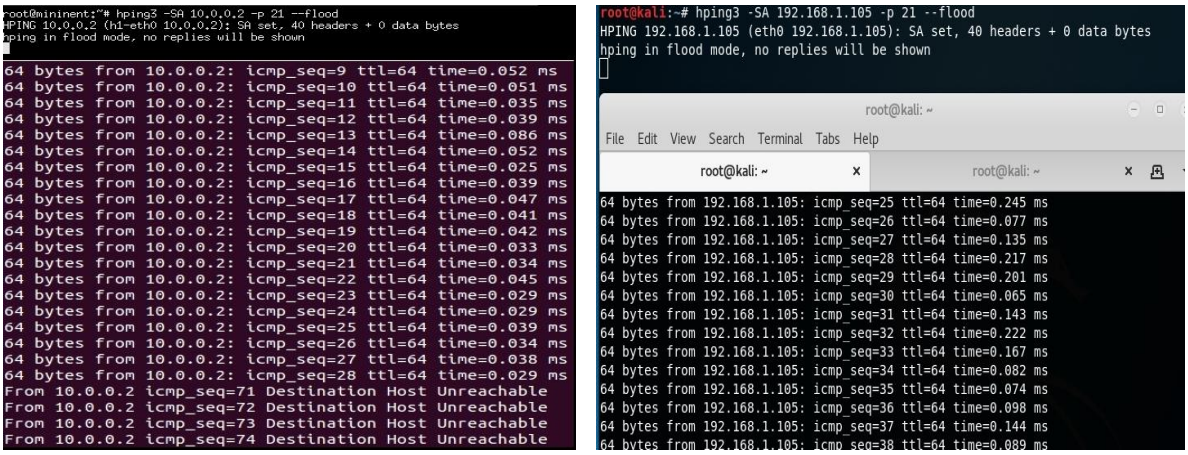


(a) yazılım tanımlı ağ (b) geleneksel bilgisayar ağı

Şekil 3. Saldırı 3 – RST/FIN Flood.

DOI: 10.34186/klujes.578590 *Geliş Tarihi:06.11.2019 Kabul Tarihi: 31.12.2019*

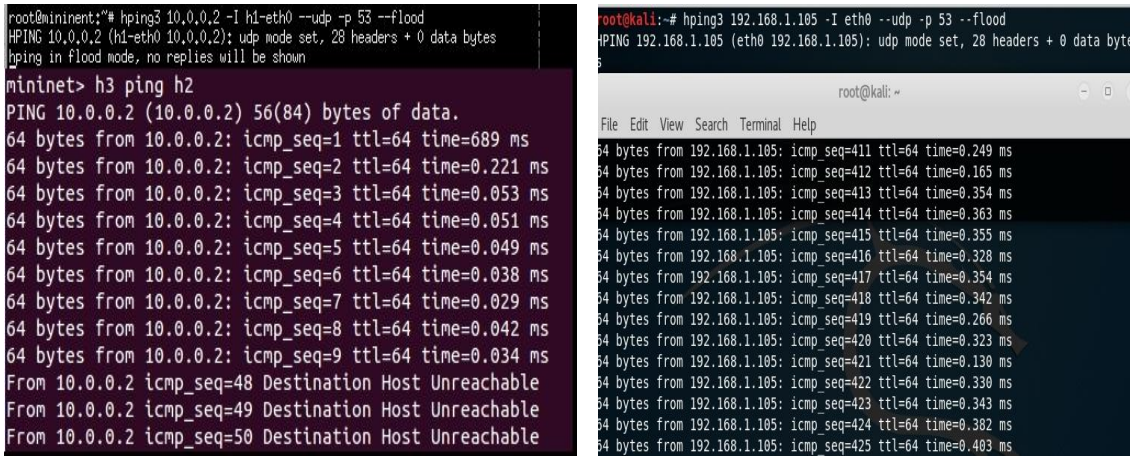
Şekil 4'te gösterildiği gibi SYN-ACK Flood saldırısı yapılan düğüm saldırı başladıktan sonra ağdan kopmuştur. Ağdan tamamen kopmadan önce birkaç defa ağa tekrar bağlanmış olsa bile sonuç değişmemiştir. Geleneksel bilgisayar ağlarında ise saldırıya maruz kalan makine saldırıdan etkilenmemiştir.



(a) yazılım tanımlı ağ (b) geleneksel bilgisayar ağı

Şekil 4. Saldırı 4 – SYN-ACK Flood.

Şekil 5'de gösterildiği gibi UDP Flood saldırısı yazılım tanımlı ağda başladıktan kısa bir süre sonra, saldırıya maruz kalan düğüm ağdan birkaç defa düşmesine rağmen ağa tekrar bağlanmayı başarmıştır. Fakat en sonunda ağdan tamamen kopmuştur. Geleneksel bilgisayar ağlarında ise saldırıya maruz kalan makine saldırıdan etkilenmemiştir.

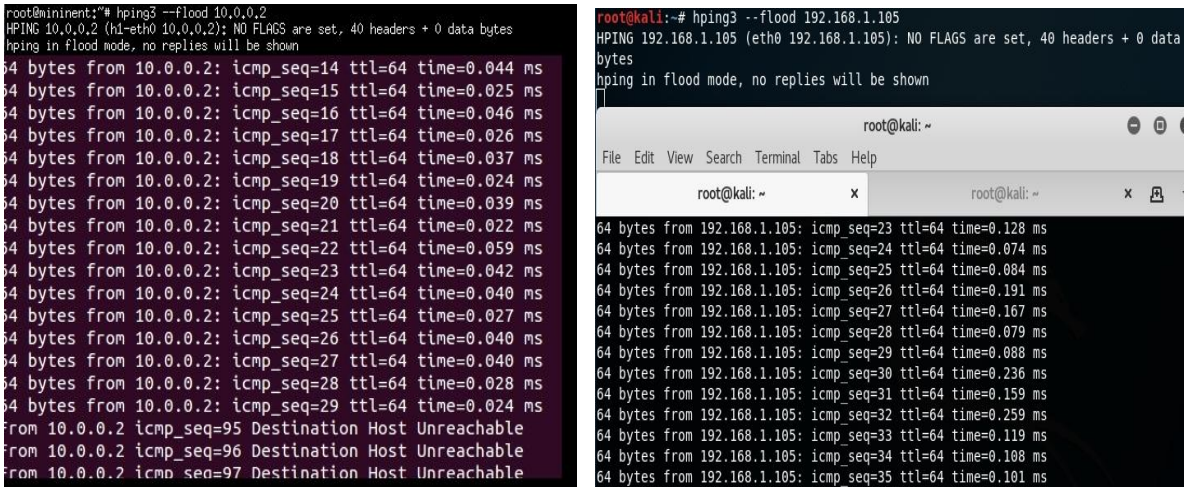


(a) yazılım tanımlı ağ (b) geleneksel bilgisayar ağı

Şekil 5. Saldırı 5 – UDP Flood.

DOI: 10.34186/klujes.578590 *Geliş Tarihi:06.11.2019 Kabul Tarihi: 31.12.2019*

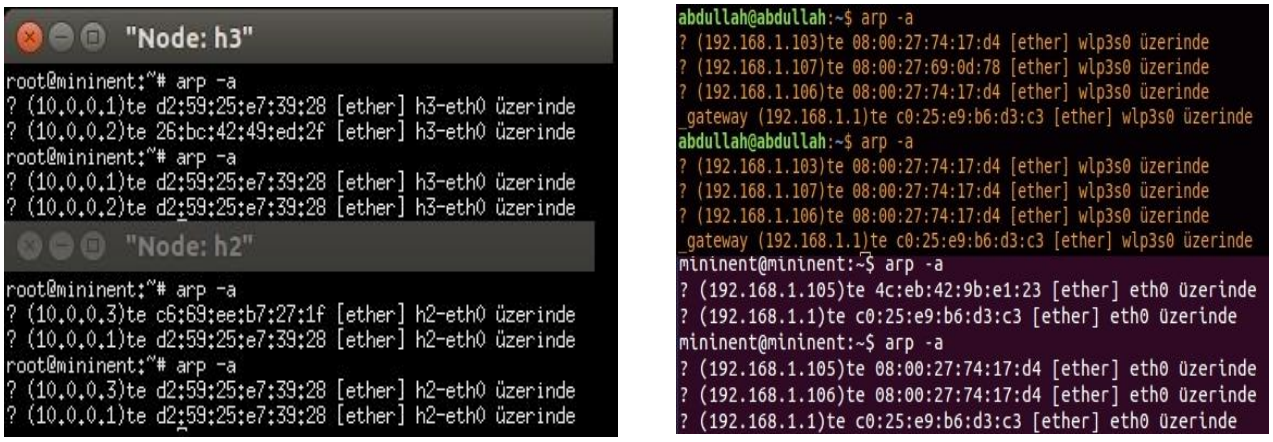
Şekil 6'da gösterildiği gibi DDoS saldırısı yazılım tanımlı ağda başladıktan sonra belirli bir süre saldırıya maruz kalan düğüm paket alımına devam etmiş fakat en sonunda ağdan tamamen kopmuştur. Geleneksel bilgisayar ağlarında yapılan saldırıda ise saldırıya maruz kalan makine saldırıdan etkilenmemiştir.



(a) yazılım tanımlı ağ (b) geleneksel bilgisayar ağı

Şekil 6. Saldırı 6 – DDoS.

Şekil 7'de gösterildiği gibi ARP Poisoning saldırısında hem yazılım tanımlı ağ hem de geleneksel bilgisayar ağı, ARP Poisoning saldırısına karşı koyamamıştır. Saldırı başladıktan hemen sonra, saldırıya maruz kalan düğüm ve makine haberleşmeyi saldırgan düğüm üzerinden devam ettirmiştir.



(a) yazılım tanımlı ağ (b) geleneksel bilgisayar ağı

Şekil 7. Saldırı 7 – ARP Poisoning.

DOI: 10.34186/klujes.578590 *Geliş Tarihi:06.11.2019 Kabul Tarihi: 31.12.2019*

Gerçekleştirilen saldırıların sonuçları genel olarak ele alındığında geleneksel bilgisayar ağları, ARP Poisoning saldırısı dışında diğer saldırılara karşı daha başarılı olurken, yazılım tanımlı ağların bütün saldırılarda başarısız olduğu ortaya çıkmıştır. Bu sonuçlar dikkate alındığında yazılım tanımlı ağların herhangi bir güvenlik tedbiri olmadan kullanımı önerilmemektedir. Ancak alınabilecek bazı tedbirler ile güvenlik sorunları minimize edilebilir. Yazılım tanımlı ağlarda olası her saldırı türüne önlem olarak kullanılabilecek bir tedbir bulunmamakla birlikte DDoS saldırılarına önlem olarak kontrol düzleminde hız sınırlama ve paket düşürme teknikleri kullanılmalıdır. ARP Poisoning saldırılarına önlem olarak ise kimlik doğrulama yöntemleri devreye alınmalıdır.

3. SONUÇLAR

Yazılım tanımlı ağlar birçok avantaja sahip olmakla birlikte bilgi güvenliği tehditleri açısından yeterince ele alınmamıştır. Bu nedenle yazılım tanımlı ağların bilgi güvenliği tehditleri açısından değerlendirilmesi büyük önem taşımaktadır. Bu çalışmada yazılım tanımlı ağların bilgi güvenliği tehditlerine karşı zafiyetleri, geleneksel bilgisayar ağlarıyla kıyaslanarak değerlendirilmiş ve çözüm önerileri sunulmuştur. Hping3 ve Dsniff uygulamaları kullanılarak gerçekleştirilen benzetim çalışmalarında IP Spoofing, SYN Flood, RST/FIN Flood, SYN-ACK Flood, UDP Flood, ARP Poisoning ve DDoS saldırıları gerçekleştirilmiştir. Gerçekleştirilen benzetim çalışmalarının sonuçları, geleneksel bilgisayar ağlarına kıyasla yazılım tanımlı ağların daha fazla güvenlik zafiyeti taşıdığı göstermekle birlikte DDoS saldırılarına önlem olarak kontrol düzleminde hız sınırlama ve paket düşürme teknikleri, ARP Poisoning saldırılarına önlem olarak ise kimlik doğrulama yöntemleri kullanılabilir. Benzetim çalışmalarına dayalı olarak gerçekleştirilen bu çalışmanın devamında, gerçek sistemler üzerinde yazılım tanımlı ağların ayrıntılı güvenlik değerlendirmeleri yapılması planlanmaktadır.

DOI: 10.34186/klujes.578590 *Geliş Tarihi:06.11.2019 Kabul Tarihi: 31.12.2019*

KAYNAKLAR

[1] Dhaya R., Maharaj S., Sownmya J., & Kanthavel R., Software Defined Networking: Viewpoint of From IP Networking, PROS and CONS and Exploration Thoughts, 2017 International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai,15-16 Haziran 2017.

[2] Kreutz D., Ramos F., Verissimo P., Rothenberg C. E., Azodolmolky S., & Uhlig S., Software-defined networking: A comprehensive survey, Proceedings of the IEEE, C 1, S 14-76, 2015.

[3] Sahba R., A Brief Study of Software Defined Networking for Cloud Computing, 2018 World Automation Congress, Stevenson, WA, 3-6 Haziran 2018.

[4] King D., Rotsos C., Aguado A., Georgalas N., & Lopez V., The Software Defined Transport Network: Fundamentals, findings and futures, 2016 18th International Conference on Transparent Optical Networks (ICTON) , Trento, 10-14 Temmuz 2016.

[5] Alparslan Ö., Veri Merkezlerinde Büyük Boyutlu Verilerin Taşınması Sürecinde Yazılım Tanımlı Ağların (SDN) Kullanımı, Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Üniversitesi, 2016.

[6] Tennenhouse ,D. Smith, J., Sincoskie W., Wetherall D., & Minden, G., A survey of active network research, IEEE Communication Magazine, C 35, S 80–86, Ocak 1997.

[7] Lazar K., Lim S., & Marconcini, F., Realizing a foundation for programmability of ATM networks with the binding architecture, Journal on Selected Areas in Communications, C 14, S 1214–1227, Eylül 1996.

[8] Sheinbein, D., & Weber, R. P., 800 service using SPC network capability, Bell System Techonology Journal, C 61, S 1737–1744, Eylül 1982.

[9] Caesar M., Design and implementation of a routing control platform, Paper presented at the 2nd Conference Symposium Network System Design Implementation, C 2, S 15–28, 2005.

[10] McKeown N., Anderson T., Balakrishnan H., Parulkar G., Peterson L., Rexford J., Shenker S., & Turner J., OpenFlow: Enabling innovation in campus networks, ACM SIGCOMM Computer Communication Review, C 38,S 69-74, Nisan 2008.

[11] Aksoy F., & Das R., Yazılım tanımlı ağlar için OMNeT++ platformunda OpenFlow protokolünün benzetimi, 2019 International Artificial Intelligence and Data Processing

DOI: 10.34186/klujes.578590 *Geliş Tarihi:06.11.2019 Kabul Tarihi: 31.12.2019*

Symposium (IDAP), Malatya, Türkiye, 21-22 Eylül 2019.

[12] https://www.opennetworking.org Erişim Tarihi: 03.10.2019.

[13] https://www.opennetworking.org/wp-content/uploads/2013/02/TR_SDN_ARCH_1.0_06062014.pdf Erişim Tarihi: 27.09.1019.

[14] Aydın M. A., Zaim A. H., & Ceylan K. G., A hybrid intrusion detection system design for computer network security, Computers and Electrical Engineering, C 35, S 517–526, 2009.

[15] Sezer, S., Scott-Hayward, S., Chouhan, P. K., Fraser, B., Lake, D., Finnegan, J., Viljoen N., Miller N. M., & Rao, N., Are We Ready for SDN? Implementation Challenges for Software-Defined Networks, IEEE Communications Magazine, C 51, S 36-43, 2013.

[16] http://www.hping.org Erişim Tarihi: 06.10.2019.

[17] https://www.monkey.org/~dugsong/dsniff/ Erişim Tarihi: 06.10.2019.

[18] http://www.projectfloodlight.org/floodlight/ Erişim Tarihi: 30.10.2019.

[19] http://mininet.org Erişim Tarihi: 30.09.2019.

[20] https://www.kali.org Erişim Tarihi: 30.10.2019.