Derin Paket Analizi Kullanılarak DDoS Saldırı Tespiti

[1]Erman Özer
[1] Department of Computer Engineering, Sakarya University
Sakarya,TURKEY

Özet

Günümüz bilişim teknolojilerinin en büyük sorunlarından biri siber saldırılardır. Bu makalede derin paket analizi kullanılarak DDoS saldırısı olup olmadığı tespit edilmiştir. Öncelikle ağ trafiği dinlenerek gelen paketler yakalanmıştır. Paketlerin türüne ve sayısına göre filtreleme işlemi yapılmıştır. Bu paketler veritabanına kaydedilerek analiz edildi, günlük değerler ve ortalama değerler bilinen saldırı desenleriyle karşılaştırıldı ve bir DDoS saldırı girişimi olup olmadığı tespit edilmiştir.

Anahtar kelimeler: Siber güvenlik, Derin paket analizi, DDoS saldırısı

Towards DDoS Attack Detection Using Deep Packet Analysis

Abstract

One of the biggest problems of today's informatics technology is cyber attacks. In this paper whether DDoS attacks will be determined by deep packet inspection. Initially packets are captured by listening of network traffic. Filtering is performed in accordance with the type and the number of packages. These packets are recorded to database to be analyzed, daily values and average values are compared by known attack patterns and will be determined whether a DDoS attack attempts.
Bu paketler veritabanına kaydedilerek analiz edilecek, günlük değerler ve ortalama değerler bilinen saldırı desenleriyle karşılaştırılacak ve bir DDoS saldırı girişimi olup olmadığı tespit edilecektir.

Key words: Cyber security, Deep packet analysis, DDoS attack

1. Giriş

Ağ trafiği dinlendiğinde çok sayıda paket elde edilmektedir. Günümüzde daha çok paket dinleyiciler kullanılarak paketler yakalanmaktadır. Paket yakalayıcı ağ üzerindeki verileri toplar. Paket dinleyiciler ise en etkili veri toplama yöntemi olarak bilinmektedir[1]. Paket dinleyiciler paket yakalamak için pcap kütüphanesini kullanırlar. Pcap kütüphanesinin windows formu winpcap iken Linux sistemlerde libpcap kütüphanesi kullanmaktadır[2,3]. Abes Damir ve arkadaşları wireshark programını kullanarak paket analizlerini yapmışlardır. Aynı şekilde Mohammed Abdul Qadeer ve arkadaşları da wireshark programını kullanmışlardır[3,4].

*Corresponding author: Address: Faculty of Engineering, Department of Computer Engineering Sakarya University, 54187, Sakarya TURKEY. E-mail address: ermanozer@sakarya.edu.tr, Phone: +902642953719

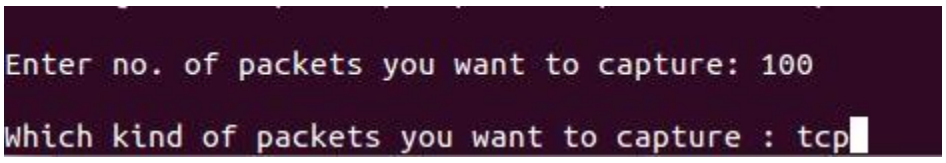
2. DDoS

Uygulama sunucuları olsun veya web sunucuları olsun veya buna benzer sunucular olsun DDoS saldırıları çevrimiçi faaliyetleri durdurabilir. DDoS saldırıları uzun süredir gerçekleşmesine rağmen bu saldırıların boyutu, sıklığı ve karmaşıklığı çoğu kurumun bu saldırıları önleme kapasitesinden çok daha hızlı artmaktadır. Saldırganlar hizmet reddi saldırısına uygun koşulları genelde sunucunun bant genişliğini tüketerek veya sunucunun kendisine zarar vererek oluştururlar. Saldırı, hedef makineye birçok istek yollanarak gerçekleştirilir. Bunun sonucunda makine normal trafiğe yanıt veremez veya pratikte devre dışı kalmış olarak kabul edilebilecek kadar yavaş yanıt verir. Guang Jin ve arkadaşları Packet Asymmetry Path Marking(PAMP) sistemini kullanarak kötü niyetli flooding trafiğini belirlemişlerdir. Kullandıkları sistem paketlerin asimetrik olarak sergilenmesidir[5]. Yen-Hun-Hu ve arkadaşları Window-Based Packet Filtering(WBPF) sistemini kullanmışlardır. Bu sistemde akış oranı normal bant genişliğinden fazla ise sistemde saldırı olduğunu tespit eder. Kuyrukta çok fazla paket olup olmadığına bakarlar[6]. Theerasak Thapngam ve arkadaşları paket varışlarını gözlemleyerek, ağ trafiğindeki davranışlarıyla çözüm bulmuşlardır. Bu teknik ile DDoS atak kaynakları ve gerçek kullanıcılar arasında ayırt etme sağlanır. Paket varış oranını kullanarak atak olup olmadığı anlaşılır[7]. You-ye Sun ve arkadaşları Deterministic Packet Marking(DPM) sistemini kullanarak DDoS atak olup olmadığını tespit etmişlerdir. Bu metotla çok sayıda eşzamanlı DDoS saldırganlarının izini sürer[8].

Bölüm 3'de yapılan metot adım adım anlatılmıştır.

3. Metot

Uygulama Linux sistem üzerinde libpcap kütüphanesi kullanılarak geliştirilmiştir. Libpcap Linux ortamları için geliştirilmiş olan (Windows kullanıcıları için ise winpcap kütüphaneleri kullanılmaktadır) ve ağ kartımız üzerinde paket yakalama, gönderme gibi işlemleri kolaylıkla yapmamıza olanak sağlayan bir kütüphanedir. Uygulama kısmında C program dilini kullanarak geliştirilen program ile ağ trafiği dinlenerek paketler yakalanmaktadır. Şekil 1'de görüldüğü gibi yakalanmak istenen paket sayısı ve paketlerin türüne göre filtrelenme işlemi yapılmıştır.



Şekil 1. Paket filtreleme

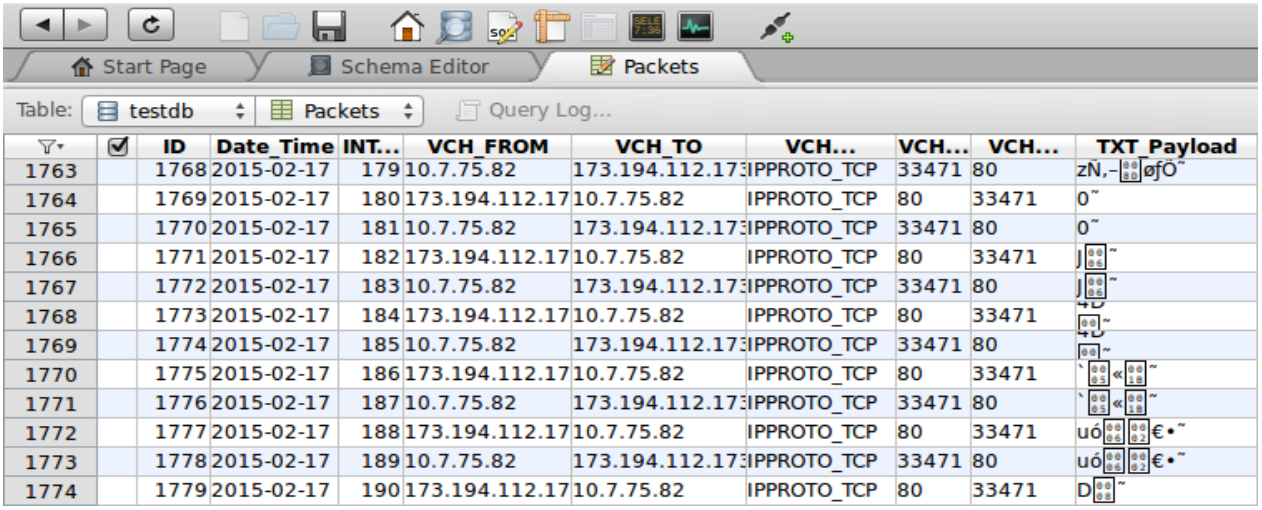
Şekil 2'de yakalanan paketlerden herhangi birinin terminaldeki görüntüsü eklenmiştir. Şekilde de görüldüğü üzere paketler; paket numarası, geldiği adres, gönderildiği adres, protokol türü, kaynak

portu, hedef portu ve payload(paket hakkındaki veri) gibi türlere göre yakalanmıştır.

```
Packet number 88:
       From: 192.168.1.34
         To: 216.58.209.3
   Protocol: TCP
   Src port: 42236
   Dst port: 443
   Payload (556 bytes):
00000   17 03 03 02 27 00 00 00  00 00 00 00 47 db 88 fa    ....'.......G...
00016   19 d7 d3 85 20 44 9c 12  61 c3 8e 79 8b bb ac 95    .... D..a..y....
00032   b8 91 02 56 25 a4 e7 9f  b5 27 21 23 30 66 2b 26    ...V%....'!#0f+&
00048   df f0 4f 88 53 62 97 0f  bf 23 a8 05 c4 fe 86 5e    ..O.Sb...#.....^
00064   e7 36 d5 eb 50 c6 6c d3  19 1d d3 4e 3a 66 d9 6c    .6..P.l....N:f.l
00080   25 1f f6 2e 06 78 d9 e5  6f 03 f9 a9 34 a2 84 c2    %....x..o...4...
00096   16 99 60 5f 38 5c 11 87  9f 46 42 d4 15 37 0b 0c    ..`_8\...FB..7..
00112   cc 43 52 b1 ea b2 59 5b  16 08 7b 94 df e7 d6 59    .CR...Y[..{....Y
00128   b6 21 ba 22 ea 72 10 a0  f1 c9 75 ae 93 89 8e d1    .!."r....u.....
00144   00 8e b0 df 12 0f be b1  92 7a 1b 15 9a ef 8f 9b    .........z......
00160   53 75 76 fa 5b 80 d7 12  f3 14 4e 1d fc e1 27 08    Suv.[.....N...'.
00176   06 5b 26 54 74 53 f1 d7  89 05 b6 f9 20 5e 47 dd    .[&TtS...... ^G.
00192   50 04 f9 30 ba 6d 7e 59  3f bd 34 8f ee 3f a9 9a    P..0.m~Y?.4..?..
00208   4e 97 10 2e 5d c4 68 78  f9 2e cb f6 55 1d 40 b8    N...].hx....U.@.
00224   e6 35 2c dc 47 ef 1b 38  62 e9 9a 0e 81 15 11 72    .5,.G..8b......r
00240   67 c0 2f 50 48 42 5a 19  87 bb ae 5e cd 31 43 3e    g./PHBZ....^.1C>
00256   fd 9c 44 90 49 db 0c 2d  a0 cc 28 5c 76 fa 52 36    ..D.I..-..(\v.R6
00272   fe f5 21 2a eb fd 1f c4  4f 91 41 12 ca bf b7 21    ..!*....O.A....!
00288   18 89 0c d0 07 80 9f 07  e8 1e 40 d1 06 d8 e3 1e    ..........@.....
```

Şekil 2. Örnek paket içeriği

Bu yakalanan ve türüne göre filtrelenen paketler Şekil 3'de görüldüğü üzere MySql veritabanına kaydedilmektedir.



		ID	Date_Time	INT...	VCH_FROM	VCH_TO	VCH...	VCH...	VCH...	TXT_Payload
1763		1768	2015-02-17	179	10.7.75.82	173.194.112.173	IPPROTO_TCP	33471	80	zN,-øfO˜
1764		1769	2015-02-17	180	173.194.112.17	10.7.75.82	IPPROTO_TCP	80	33471	0˜
1765		1770	2015-02-17	181	10.7.75.82	173.194.112.173	IPPROTO_TCP	33471	80	0˜
1766		1771	2015-02-17	182	173.194.112.17	10.7.75.82	IPPROTO_TCP	80	33471	J˜
1767		1772	2015-02-17	183	10.7.75.82	173.194.112.173	IPPROTO_TCP	33471	80	J˜
1768		1773	2015-02-17	184	173.194.112.17	10.7.75.82	IPPROTO_TCP	80	33471	˜
1769		1774	2015-02-17	185	10.7.75.82	173.194.112.173	IPPROTO_TCP	33471	80	˜
1770		1775	2015-02-17	186	173.194.112.17	10.7.75.82	IPPROTO_TCP	80	33471	`«˜
1771		1776	2015-02-17	187	10.7.75.82	173.194.112.173	IPPROTO_TCP	33471	80	`«˜
1772		1777	2015-02-17	188	173.194.112.17	10.7.75.82	IPPROTO_TCP	80	33471	uó€•˜
1773		1778	2015-02-17	189	10.7.75.82	173.194.112.173	IPPROTO_TCP	33471	80	uó€•˜
1774		1779	2015-02-17	190	173.194.112.17	10.7.75.82	IPPROTO_TCP	80	33471	D˜

Şekil 3. Veritabanı

Sistemde 13 günlük verilerin analizi yapılmıştır. Gün bazlı olarak paket sayıları kontrol edilmiştir. Toplam paket sayısı ve ortalama paket sayısı belirlendikten sonra, günlük olarak yakalanan paket sayıları arasında kıyaslama yapılmıştır. Saldırı tespit edildiğinde system çalışmayı durdurmaktadır. Şekil 4' te hem kıyaslama işlemi hem de DDoS saldırısı olup olmadığı tespit edilmiştir.

Toplam Paket Sayısı : 3217

Günler => PaketSayısı
22 - 02 => 100
04 - 02 => 588
24 - 02 => 150
06 - 02 => 217
25 - 02 => 35
13 - 02 => 15
27 - 02 => 170
16 - 02 => 530
17 - 02 => 495
18 - 02 => 13
21 - 02 => 70
02 - 03 => 720
10 - 03 => 114

Ortalama paket sayısı : 247.46153846154
Günler => PaketSayısı
22 - 02 => 100
04 - 02 => 588 **DDOS ATAK TESBİT EDİLMİŞTİR !!!**
24 - 02 => 150
06 - 02 => 217
25 - 02 => 35
13 - 02 => 15
27 - 02 => 170
16 - 02 => 530 **DDOS ATAK TESBİT EDİLMİŞTİR !!!**
17 - 02 => 495 **DDOS ATAK TESBİT EDİLMİŞTİR !!!**
18 - 02 => 13
21 - 02 => 70
02 - 03 => 720 **DDOS ATAK TESBİT EDİLMİŞTİR !!!**
10 - 03 => 114

Şekil 3. Saldırı tespiti

Şekilde de görüldüğü üzere "4 Şubat 2015", "16 Şubat 2015", "17 Şubat 2015" ve "2 Mart 2015" tarihinde yakalanan paketler ortalamanın bayağı üzerindedir. Şekilden anlaşıldığı üzere belirtilen günlerde saldırı tespit edilmiştir.

4.Sonuç

Bu çalışmada libpcap kütüphanesi kullanılarak ağ trafiği dinlenmiştir ve paket yakalama, paket gönderme işlemleri gerçekleştirilmiştir. İstenilen sayıda ve istenilen türde paket filtreleme işlemi yapılmıştır. Filtreleme işlemi yapıldıktan sonra yakalanan paketler veritabanına kaydedildikten sonra analiz edilerek saldırı olup olmadığı tespit edilmiştir.

Kaynaklar

1. Kumar, G.D.; Guru Rao, C.V.; Singh, M.K.; Ahmad, F., "Using Jpcap API to Monitor, Analyze, and Report Network Traffic for DDoS Attacks," Computational Science and Its Applications (ICCSA), 2014 14th International Conference on , vol., no., pp.35,39, June 30 2014-July 3 2014
2. Zhenqi Wang; Dankai Zhang, "Research on WinPcap Capture IPv6 Packet Method," Computer Sciences and Applications (CSA), 2013 International Conference on , vol., no., pp.94,97, 14-15 Dec. 2013
3. Qadeer, M.A.; Zahid, M.; Iqbal, A.; Siddiqui, M.R., "Network Traffic Analysis and Intrusion Detection Using Packet Sniffer," Communication Software and Networks, 2010. ICCSN '10. Second International Conference on , vol., no., pp.313,317, 26-28 Feb. 2010
4. Dabir, A.; Matrawy, A., "Bottleneck Analysis of Traffic Monitoring using Wireshark," Innovations in Information Technology, 2007. IIT '07. 4th International Conference on , vol., no., pp.158,162, 18-20 Nov. 2007
5. Guang Jin; Jiangang Yang; Wei Wei; Yabo Dong, "Resisting Network DDoS Attacks by Packet Asymmetry Path Marking," Communications and Networking in China, 2007. CHINACOM '07. Second International Conference on , vol., no., pp.1205,1209, 22-24 Aug. 2007
6. Yen-Hung Hu; Hongsik Choi; Choi, H.-A., "Packet filtering to defend flooding-based DDoS attacks [Internet denial-of-service attacks]," Advances in Wired and Wireless Communication, 2004 IEEE/Sarnoff Symposium on , vol., no., pp.39,42, 26-27 Apr 2004
7. Thapngam, T.; Shui Yu; Wanlei Zhou; Beliakov, G., "Discriminating DDoS attack traffic from flash crowd through packet arrival patterns," Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on , vol., no., pp.952,957, 10-15 April 2011
8. You-ye Sun; Cui Zhang; Shao-qing Meng; Kai-ning Lu, "Modified Deterministic Packet Marking for DDoS Attack Traceback in IPv6 Network," Computer and Information Technology (CIT), 2011 IEEE 11th International Conference on , vol., no., pp.245,248, Aug. 31 2011-Sept. 2 2011