C0R3 Bilişim Güvenliği Grubu

Saldırı Tespit ve Tehlike Yönetim Sistemleri (IDS & TMS)

Evrim ULU <evrim@core.gen.tr>
Aycan İRİCAN <aycan@core.gen.tr>

”People who know little are generally good talkers, while people who know much say little.”
- Jean Jaques Rousseau

Saldırı Tespit Sistemleri

- Kalıp Eşleştirme Sistemleri
  - Snort vs.
- Anormallik Algılayıcı Sistemler
  - Cylant Secure, NFR(Network Flight Recorder) vs.

Saldırı Tespit Sistemleri

- Yerel Sistemler, Sistem Bazlı
- Dağınık Sistemler

Algılayıcı ve İşleyiciler

- Algılayıcı: Olayın olduğu veya olayın ilk olarak algılandığı ortamdır. Algılayıcı ağa bağlı bir bilgisayar yada bir geçit olabilir.
- İşleyici: Algılayıcıdan alınan bilgilerin veritabanındaki bilgilerle karşılaştırarak saldırının tespit edildiği yerdir.
- Veritabanı: Algılayıcının verileri depoladığı, işleyicinin de değerlendirmek üzere verileri aldığı ortamdır.

Algılayıcı

- Ağdan gelen paketlerin ve sistemde cereyan eden olayların ilk değerlendirildiği yerdir.
- İşleyicinin görevlerini azaltmak için süzgeçlik görevi görür.
- Gerektiğinde saldırıya karşı önlem alabilecek nitelikte ve sistem ile iç içe olmalıdırlar.

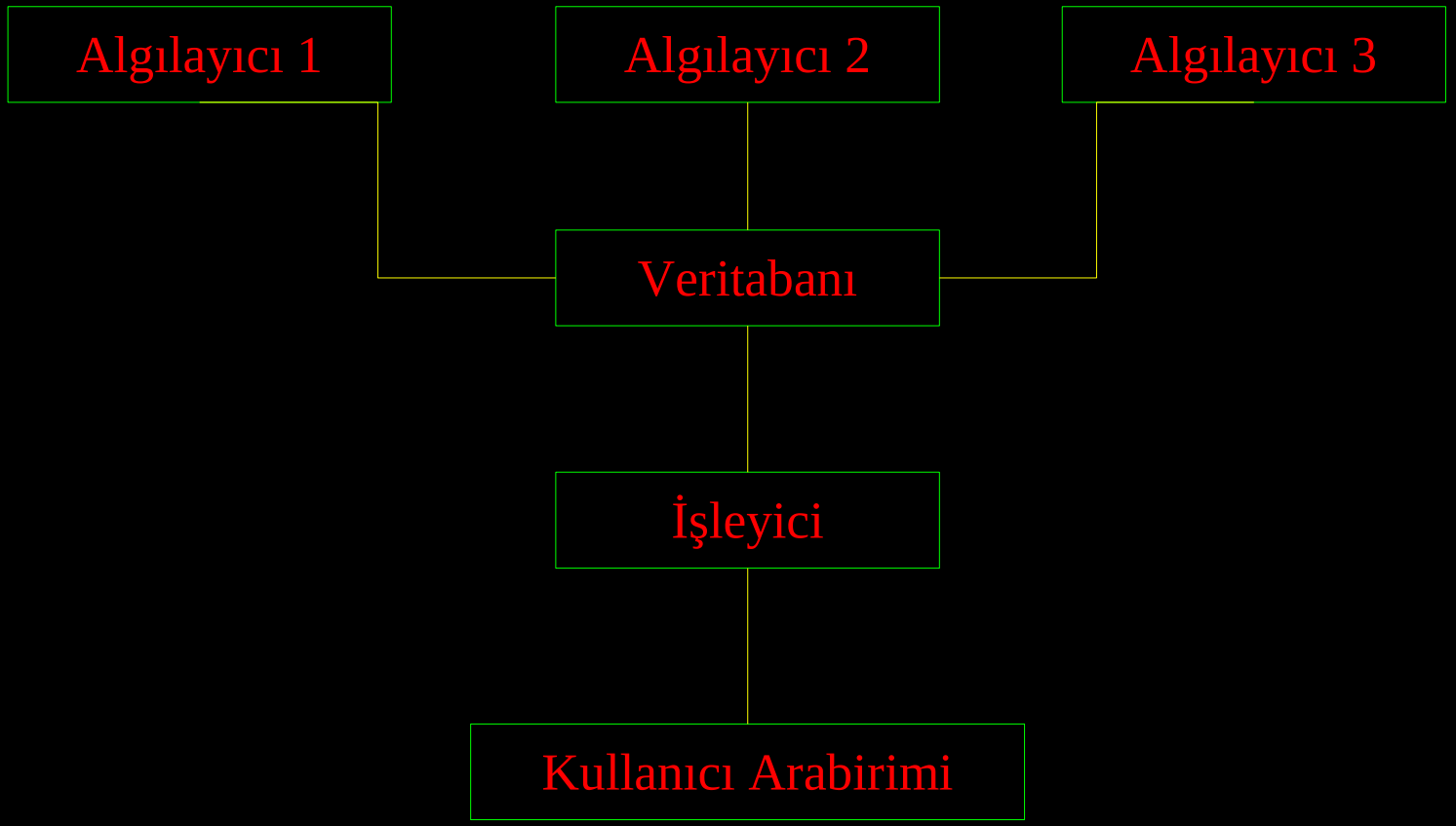
İşleyici

- Veritabanında toplanan verileri eş zamanlı olarak işleyen, karşılaştıran sistemdir.
- Ağın boyutuna göre işlevlerini yerine getirebilmeleri için güçlü makinalara ihtiyaç duyabilirler.
- Kullanıcı arabirimi ile sistem yöneticisini uyarabilir veya önceden belirlenmiş otomatik hareketlerden birini gerçekleştirebilirler.

Veritabanı

- Algılayıcılardan aldığı verileri işlenmek üzere saklar.
- Saldırı sisteminin tüzüğüne göre verileri düzelner ve eskimiş olanları siler.
- İşleyicinin direktiflerine göre bazı verileri daha sonra yeniden değerlendirmek üzere aylarca saklayabilir.

Dağınık STS Yapısı



Kalıp Bazlı Saldırı Tespit Sistemleri

- Önceden tespit edilmiş saldırıların eş zamanlı olarak işleyici tarafından karşılaştırılmasını esas alır.
- Her saldırı için kalıp veritabanında bulunmalıdır.
- Yeni çıkan saldırı tiplerinin otomatik olarak veritabanına girilmesi gerekir (Ör: Anti-virüs sunucuları).

Anormallik Algılayıcı Sistemler

- Belli bir süre sadece sistemi izlerler ve sistemin çalışmasını istatistiksel olarak modellerler.
- Öğrenme süreçlerinde kalıp bilgilerini sistemin normal davranışlarından çıkarırlar.
- Her türlü sistem bilgisini kayıt edebilirler (Ör: saatlik işlemci kullanımı, kullanıcı sayısı, yüklü yazılımlar, komut argümanları).
- Öğrenme süreleri sistemden sisteme değişebilir.

Anormallik Algılayıcı Sistemler

- Öğrenme süreci sonunda çalışma sürecine girerler.
- Kalıp karşılaştırma yerine önceden kurdukları modele dayanarak sistemin normal davranışı dışındaki hareketleri izlerler.
- Sistem modeline göre eşik değeri üzerindeki işlemler anormallik olarak algılanır ve tanımlanmış önlem alınır.

Anormallik Algılayıcı Sistemler

- Saldırganın tespitinin ardından yapabilecekleri birçok işlem vardır.
- Sistem yöneticisini uyarabilirler.
- Saldırının yapıldığı bilgisayar ile ağ bağlantısı belirlenen bir süre kesilebilir.
- Anormal olarak algılanan süreç sonlandırılabilir.
- Saldırıyı kaydedip izleyebilirler.

Toplanan Veriler

- Protokol Bilgileri: IP başlığı, TCP/UDP başlıkları
- Transfer edilen veri boyutu
- Sistemde çalışan servisler (SMTP, SNMP, HTTP vs.)
- Sistemde yüklü olan yazılımlar
- Kullanıcı bilgileri (sistem yöneticisi, bölüm şefi)

Toplanan Veriler

- Kullanıcıların kullandıkları yazılımlar
- Hangi saatler arasında bağlı kaldıkları
- Ne kadar işlemci/bellek kullandıkları
- Aylık/günlük ağ trafik yoğunluğu

Saldırı Tespit Sonrası

- Saldırı tespit edildikten sonra sistem
- Sistem yöneticisini uyarabilir,
- Saldırgan sistem ile bağlantıyı ana ateş duvarından kesebilir,
- Saldırıyı izleyip kaydedebilir.

Sistem Elemanlarının Haberleşmesi

- Algılayıcı, veritabanı ve işleyici birbiriyle protokol seviyesinde güvenli haberleşmelidirler.
- Bunun için ikili anahtar sistemi kullanılabilir.
- Veritabanındaki bilgiler şifrelenmelidir. Aksi takdirde veritabanının istismar edilmesi durumunda tümö sistem saldırgan tarafından ele geçirilebilir.

Tehlike Sadece Dışarıda mı?

- Saldırı tespit sistemleri genellikle dışarıdan gelebilecek saldırılara karşı donanımlıdır.
- Buna karşın birçok firma içerisinde çalışan kişiler haklarını istismar ederek sisteme zarar vermeye çalışabilirler.
- Bu yüzden kullanıcı hakları da denetlenmelidir. Birden sistem yöneticisi haklarına sahip mühendis algılandığında sistem uyarı vermelidir.

Linux Saldırı Tespit Sistemleri

- Kalıp bazlı saldırı tespit sistemi
  - Snort
- Anormallik algılayıcı sistem
  - Cylant Secure

SNORT (1)

- Martin Roesch , GPL
- Ağ Saldırı Tespit Sistemi
- Genel olarak 3 işlevi var. Bunlar:
  - Tcpdump alternatifi (sniffer)
  - paket günlüğü (logger)
  - ağ saldırı tespit sistemi (NIDS)
- Eklentiler (plugins)
- Demarc

SNORT – sniffer (1)

```
Infinity root # snort -ilo -qv

05/11-22:22:55.043039 127.0.0.1:32775 -> 127.0.0.1:23
TCP TTL:64 TOS:0x10 ID:56674 IpLen:20 DgmLen:60 DF
12****S* Seq: 0xFF519BDC  Ack: 0x0  Win: 0x7FFF  TcpLen: 40
TCP Options (5) => MSS: 16396 SackOK TS: 345790 0 NOP WS: 0
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

05/11-22:22:55.043070 127.0.0.1:23 -> 127.0.0.1:32775
TCP TTL:255 TOS:0x10 ID:0 IpLen:20 DgmLen:40 DF
***A*R** Seq: 0x0  Ack: 0xFF519BDD  Win: 0x0  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

```
Bash$ telnet 0 23
Trying 0.0.0.0...
telnet: Unable to connect to remote host: Connection refused
```

SNORT – sniffer (2)

```
Infinity root # snort -ilo -qvd
05/11-22:35:21.162921 127.0.0.1:22 -> 127.0.0.1:32778
TCP TTL:64 TOS:0x2 ID:50732 IpLen:20 DgmLen:75 DF
***AP*** Seq: 0x2F07AC1E  Ack: 0x2F71B9EB  Win: 0x7FFF  TcpLen: 32
TCP Options (3) => NOP NOP TS: 420402 420402
53 53 48 2D 31 2E 39 39 2D 4F 70 65 6E 53 53 48      SSH-1.99-OpenSSH
5F 33 2E 31 70 31 0A                                 _3.1p1.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

05/11-22:35:21.162960 127.0.0.1:32778 -> 127.0.0.1:22
TCP TTL:64 TOS:0x10 ID:54234 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x2F71B9EB  Ack: 0x2F07AC35  Win: 0x7FFF  TcpLen: 32
TCP Options (3) => NOP NOP TS: 420402 420402

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

```
bash$ telnet 0 22
Trying 0.0.0.0...
Connected to 0.
Escape character is '^]'.
SSH-1.99-OpenSSH_3.1p1
```

SNORT – paket günlüğü

```
infinity root # mkdir yngwie
infinity root # snort -ql ./yngwie -r /mnt/core_collect/snif_logs/hu-bil1
infinity root # ls yngwie/
0.0.0.0        193.140.223.134  193.140.225.60   193.140.232.151  193.140.234.220  193.140.237.13
0.1.193.140    193.140.223.135  193.140.225.74   193.140.232.170  193.140.234.221  193.140.237.136
0.124.193.140  193.140.223.136  193.140.225.99   193.140.232.190  193.140.234.222  193.140.237.50
155.223.64.2   193.140.223.197  193.140.228.1    193.140.232.20   193.140.234.223  193.140.237.57
160.75.79.124  193.140.223.200  193.140.228.10   193.140.232.201  193.140.234.224  193.140.237.58
ARP

infinity root # ls yngwie/193.140.236.66/TCP*21
yngwie/193.140.236.66/TCP:1963-21  yngwie/193.140.236.66/TCP:1972-21
yngwie/193.140.236.66/TCP:1965-21  yngwie/193.140.236.66/TCP:1974-21
```

SNORT – ASTS (1)

```
Infinity root # snort -qd -h 192.168.31.0/24 -c /etc/snort/snort.conf -r /mnt/mp3/snif/sn1
infinity root # ls /var/log/snort/
193.140.236.31  193.140.236.66  193.140.236.70  193.140.236.74  193.140.236.78  213.248.141.27
193.140.236.60  193.140.236.68  193.140.236.71  193.140.236.75  193.140.236.79  216.244.139.242
193.140.236.61  193.140.236.69  193.140.236.72  193.140.236.76  212.82.192.72   alert
193.140.236.65  193.140.236.7   193.140.236.73  193.140.236.77  213.14.43.47    portscan.log
```

```
infinity root # cat /var/log/snort/193.140.236.75/SESSION\:3215-80
GET /config/login_verify2?.tries=1&.done=http://edit.yahoo.com
/config/mail&.src=ym&.slogin=penbem&.partner=&.intl=us&.fUpdate=&.prelog=&.bid=&.aucid=&.challenge=KsvqYBU3cjxQMAk
Jd3Hz9hlr5cLt&passwd=b8a3e935ee2a0a518d9d9bd862793c1a&lsq=ls_q_1001&ls_q_1001=&Login=Continue&.hash=1&.js=1&.m
d5=1 1 HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-powerpoint, application/vnd.ms-excel,
application/msword, */*
Accept-Language: tr
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Host: login.yahoo.com
Connection: Keep-Alive
Cookie: B=fgn3fnkubst9v&b=2; Q=q1=AACAAAAAAAAAeg--&q2=PL4iYg--;
Y=v=1&n=8ab4tq5kr86ur&l=f4d14c/o&p=f2jvvtr1103u0400&ig=1n8c8&iz=06795&r=8u&lg=us&intl=us;
T=z=8Wnv8A8c8v8AfOJJD1nxqXkNTY1BjU3Nk8zTzdOTzU-
&a=QAE&sk=DAAEyr6Sw9kdVP&d=c2wBTWpFeUFUSXdNVGcwT0RBNU9ESS0BYQFRQUUBenoBOFdudjhBZ1dB&af=QSt
BQmdBJnRzPTEwMTkxMTQ5NDAmcHM9elY2dGhiY1BUUkQ0MHh1aDEwUmttdy0t; I=ir=9f&in=11cdd7f0&i1=AAACE1E3;
C=mg=1
```

SNORT – ASTS (2)

```
Infinity root # tail -n25 /var/log/snort/alert

[**] [1:466:1] ICMP L3retriever Ping [**]
[Classification: Attempted Information Leak] [Priority: 2]
04/19-16:17:48.263340 193.140.236.68 -> 193.140.236.7
ICMP TTL:32 TOS:0x0 ID:34810 IpLen:20 DgmLen:60
Type:8  Code:0  ID:512   Seq:16896  ECHO
[Xref => http://www.whitehats.com/info/IDS311]

[**] [100:3:1] spp_portscan: End of portscan from 193.140.236.75: TOTAL time(28s) hosts(14) TCP(11) UDP(0) [**]
05/11-23:48:24.546639

[**] [1:469:1] ICMP PING NMAP [**]
[Classification: Attempted Information Leak] [Priority: 2]
04/19-16:17:51.362860 193.140.236.77 -> 193.140.236.7
ICMP TTL:128 TOS:0x0 ID:10283 IpLen:20 DgmLen:28
Type:8  Code:0  ID:512   Seq:17408  ECHO
[Xref => http://www.whitehats.com/info/IDS162]

[**] [1:469:1] ICMP PING NMAP [**]
[Classification: Attempted Information Leak] [Priority: 2]
04/19-16:18:00.438355 193.140.236.77 -> 193.140.236.7
ICMP TTL:128 TOS:0x0 ID:18125 IpLen:20 DgmLen:28
Type:8  Code:0  ID:512   Seq:17664  ECHO
[Xref => http://www.whitehats.com/info/IDS162]
```

SNORT – ASTS (3)

- Alarm türleri:
  - fast (zaman, alarm mesajı, IP bilgisi)
  - full (öntanımlı)
  - unsock (unix soketi kullanımı)
  - None (alarmı kapat)
  - Console (fast türü konsola çıktı)
- “-s” syslog
  - facilities: LOG_AUTHPRIV, LOG_ALERT
- SMB winpopup alarm türü

Cylant Secure

- Sunucları korumak için kernel eklentisi ve uygulamaları ile bir cözüm sunuyor.
- Kalibrasyon aşamasında sistem normalde hangi amaçla kullanılacaksa öyle kullanılıyor.
- Kalibrasyon bitince limitler belirleniyor.
- Çalışma esnasında limiti aşan olay için önlem alınıyor.
- Paralı bir ürün.