ΚΕΦΑΛΑΙΟ 2
ΤΟ HONEYD

Εισαγωγή

Τα τελευταία χρόνια ο όγκος της κακόβουλης διαδικτυακής κίνησης έχει αυξηθεί εντυπωσιακά, λόγω της συνεχούς εξάπλωσης των worms, τη δραστηριότητα των script kiddies που χρησιμοποιούν αυτοματοποιημένα εργαλεία για να πραγματοποιήσουν επιθέσεις, όπως port scanners, autorooters κα. Είναι ιδιαίτερα σημαντικό να μπορούμε να συγκεντρώσουμε αυτή την κίνηση και να την αναλύσουμε, καθώς μπορεί να μας διδάξει ποιές είναι οι τελευταίες εξελίξεις από την πλευρά των κακόβουλων ενεργειών, μπορεί να μας βοηθήσει να ανακαλύψουμε καινούργια είδη επιθέσεων, να δούμε ποιοι τύποι επιθέσεων και ποια worms είναι ενεργά, αλλά και να ευαισθητοποιήσει σε θέματα ασφάλειας δικτύων.

Το honeyd[1] είναι ένα εργαλείο για τη δημιουργία virtual hosts που προσομοιώνει σχεδόν οποιοδήποτε γνωστό λειτουργικό σύστημα στο επίπεδο δικτύου. Το honeyd το πετυχαίνει αυτό με το να προσομοιώνει τη στοίβα δικτύου-network stack-από τα περισσότερα λειτουργικά συστήματα και έτσι καταφέρνει να δημιουργήσει virtual hosts που φαίνονται σαν φυσικά συστήματα.

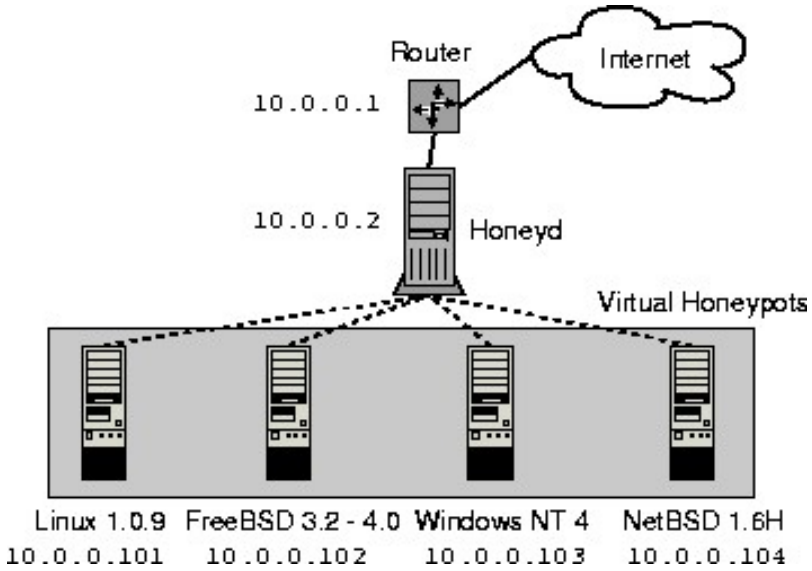
Μπορεί να έχει πολλές εφαρμογές στον τομέα της ασφάλειας δικτύων, όπως να μας δείξει μια εικόνα του τι συμβαίνει στο δίκτυο μας, να βοηθήσει να μελετήσουμε τις τεχνικές που χρησιμοποιούνται για την παραβίαση των συστημάτων, να συγκεντρώσει δεδομένα από δικτυακές επιθέσεις, να ευαισθητοποιήσει σε θέματα ασφάλειας δικτύων και ακόμα, να μπερδεύει και να αποθαρρύνει τους εισβολείς και να ενεργεί active defense ενάντια σε worms.

Το honeyd[2]

Είναι ένας μικρός open source daemon για τη δημιουργία virtual hosts σε ένα δίκτυο. Τα virtual hosts μπορούν να ρυθμιστούν να τρέχουν διάφορες υπηρεσίες και η συμπεριφορά τους μπορεί να ρυθμιστεί έτσι ώστε να προσημειώνουν διάφορα λειτουργικά συστήματα. Αυτό που κάνει το honeyd είναι να παίρνει τα network stacks διάφορων λειτουργικών συστημάτων από το fingerprint database του nmap και του Xprobe και με αυτό τον τρόπο καταφέρνει να προσομοιώσει τα αντίστοιχα λειτουργικά σε κάποιον virtual host.

Πέρα από τη χρήση του σαν εκπαιδευτικό εργαλείο για την προσομοίωση δικτύων και αυθαίρετων τοπολογιών που μπορούμε να δημιουργήσουμε εύκολα, πρόκειται για μια

πλατφόρμα για τη δημιουργία virtual honeypots, τα οποία τρέχουν εικονικά στο μηχάνημα στο οποίο εγκαθίσταται το honeyd. Μπορεί να παρέχει διαφορετικές –ανάλογα με τη ρύθμιση- τοπολογίες δρομολόγησης και υπηρεσίες για οποιονδήποτε αριθμό εικονικών συστημάτων.



Εικόνα 2.1-δημιουργία 4 virtual hosts από έναν honeyd host

Εφαρμογές

- Να πάρουμε μια εικόνα σχετικά με τις επιθέσεις που συμβαίνουν στο δίκτυο μας Να μελετήσουμε τις τεχνικές που χρησιμοποιούνται για το σπάσιμο της ασφάλειας, ώστε να μπορούμε να προστατεύσουμε καλύτερα τα συστήματα μας.
- Να συγκεντρώσουμε δεδομένα από τους επιτιθέμενους.
- Να αποθαρύνουμε τους επιτιθέμενους από το να συνεχίσουν να επιτίθενται στο δίκτυο μας.
- Να κατανοήσουμε πόσο ευπαθή είναι τα συστήματα που συνδέονται στο internet.
- Να ευαισθητοποιήσουμε για θέματα ασφάλειας δικτύων.
- Το honeyd είναι χρήσιμο στην έρευνα για την καταπολέμηση των worms και στην μάχη ενάντια στο spam email.

Λειτουργία honeyd

Το honeyd προσομοιώνει την TCP/IP στοίβα διαφόρων λειτουργικών συστημάτων , κάνοντας έτσι το virtual honeypot να φαίνεται ότι είναι μηχάνημα που τρέχει αυτό το λειτουργικό. Επίσης προσομοιώνει υπηρεσίες (πχ web, ssh, telnet) αν και αυτές δεν τρέχουν πραγματικά -μερικές από αυτές πχ εμφανίζουν ένα ενημερωτικό banner ότι πρόκειται για κάποια υπηρεσία και κατόπιν κλείνουν. Είναι πάντως αρκετά για να πείσουν έναν επιτιθέμενο να πραγματοποιήσει την επίθεση του, η αν πρόκειται για αυτοματοποιημένο εργαλείο να

ολοκληρώσει τη σύνδεση του.

Το κύριο μειονέκτημα πάντως στο γεγονός ότι οι επιτιθέμενοι αλληλεπιδρούν με τους virtual hosts μόνο στο επίπεδο δικτύου είναι ότι δεν μπορούν να αποκτήσουν πλήρη πρόσβαση στο σύστημα, ακόμα κι αν παραβιάσουν κάποια υπηρεσία.

Εκτός από virtual hosts το honeyd είναι σε θέση να δημιουργεί τις δικτυακές τοπολογίες που προσδιορίζουμε [6]. Στα virtual networks που δημιουργεί, χαρακτηριστικά όπως latency, packet loss, αλλά και φυσικά τα hops και η τοπολογία του δικτύου με την προσθήκη εικονικών routers μπορούν να ρυθμιστούν, κάνοντας έτσι το virtual network να μοιάζει όσο περισσότερο με ένα πραγματικό δίκτυο. Εργαλεία για network maping, δηλαδή εύρεση της τοπολογίας ενός δικτύου όπως το traceroute θα δείξουν τις αυθαίρετες τοπολογίες που έχουμε ορίσει. Επιπλέον μπορεί να δημιουργεί GRE[3] κανάλια, για τη δημιουργία κατανεμημένων δικτύων.

Τις παραπάνω δουλειές πραγματοποιεί το personality engine που διαθέτει το honeyd και το οποίο αποτελεί τον πυρήνα του. Το honeyd επιπλέον παρέχει τη δυνατότητα για redirection μιας σύνδεσης, είτε σε κάποιο άλλο μηχάνημα (πχ κάποιο high interactive honeypot) είτε ακόμα και στον originating host!

Το honeyd διαθέτει fingerprints database για προσομείωση του network stack για τα παρακάτω λειτουργικά συστήματα: Windows NT,XP,2000,95,98, Mac OS X, Solaris 2.6-2.7, suse8.0, cray, Linux 2.6, 2.2 ,Freebsd 5.0-5.1, Solaris 8 , openbsd 3.0-3.4 καθώς επίσης και για πολλά άλλα.

Παράδειγμα fingerprint λειτουργικού συστήματος

Ένα παράδειγμα nmap fingerprint που προσδιορίζει τη συμπεριφορά της δικτυακής στοίβας για ένα σύστημα με το λειτουργικό Microsoft Windows NT4.0 SP3, είναι το εξής:

Fingerprint Microsoft Windows NT 4.0 SP3 Class Microsoft | Windows | NT/2K/XP | general purpose
TSeq(Class=TD|RI%gcd=<18%SI=<2A00DA&>6B73)
T1(DF=Y%W=7FFF|2017%ACK=S++%Flags=AS%Ops=M|MNWNNT)
T2(Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)
T3(Resp=Y%DF=Y%W=7FFF|2017%ACK=S++|O%Flags=AS|A%Ops=M|NNT)
T4(DF=N%W=0%ACK=O|S%Flags=R%Ops=) T5(DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(DF=N%W=0%ACK=O|S++%Flags=R%Ops=) T7(DF=N%W=0%ACK=S++%Flags=AR%Ops=)
PU(TOS=0%IPLEN=38%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%DAT=E)

όπου Tseq είναι το TCP sequenceability test
T1 είναι ένα SYN πακέτο με TCP επιλογές για να ανοίξει η πόρτα
T2 είναι ένα πακέτο NULL
T3 είναι ένα πακέτο SYN|FIN|URG|PSH
T4 είναι ένα ACK

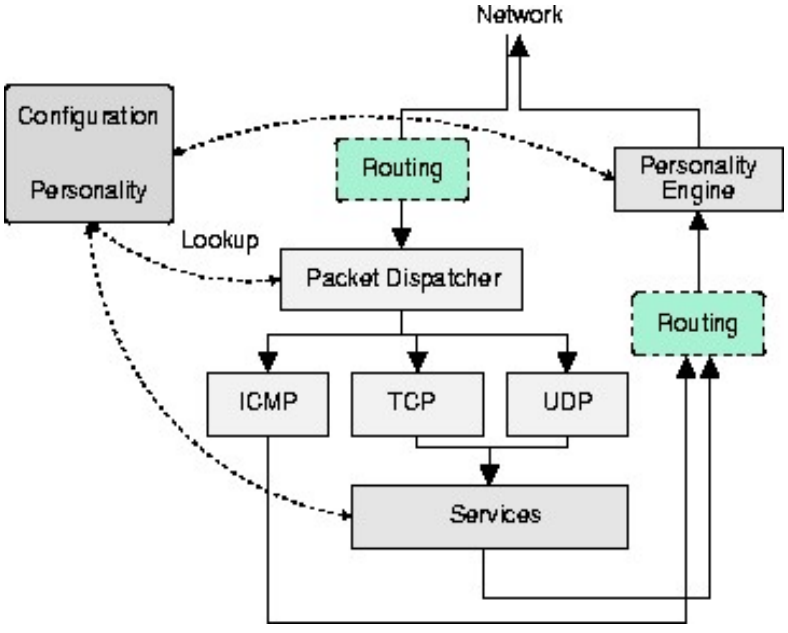
T5 είναι ένα SYN
T5 είναι ένα SYN
T6 είναι ένα ACK
T7 είναι ένα FIN|PSH|URG
PU είναι ένα UDP πακέτο

Το παράδειγμα είναι από τη βάση δεδομένων του nmap που περιέχει fingerprints από σχεδόν όλα τα γνωστά λειτουργικά συστήματα. Το fingerprint είναι κάτι σαν το δικτυακό αποτύπωμα ενός λειτουργικού συστήματος, με το οποίο στέλνει τα πακέτα στο δίκτυο για να επικοινωνεί δικτυακά. Κάθε λειτουργικό σύστημα έχει το δικό του fingerprint και από αυτό μπορούμε να αναγνωρίσουμε το λειτουργικό σύστημα αυτό, με μια τεχνική που είναι γνωστή ως port scanning. Τα port scanners ανοίγουν σύνδεση με διάφορες πόρτες του συστήματος το οποίο κάνουμε scan και από την απόκριση καταλαβαίνουν ποιες πόρτες είναι ανοικτές και τι λειτουργικό σύστημα έχει. Το πιο διάσημο port scanner είναι το nmap [4].

Αρχιτεκτονική

Η εικόνα 2.3 δείχνει την αρχιτεκτονική του honeyd, η οποία αποτελείται από τα εξής στοιχεία: configuration database, central packet dispatcher, protocol handlers, personality engine, και τέλος ένα optional routing component.

Προτού ένα πακέτο σταλεί στο δίκτυο, η personality engine τροποποιεί το περιεχόμενο του ώστε να φαίνεται ότι προέρχεται από τη δικτυακή στοίβα του λειτουργικού συστήματος το οποίο έχει ρυθμιστεί να προσομοιώνει ο virtual host.



Εικόνα 2.3-περίληψη τως αρχιτεκτονικής του honeyd

personality engine

Το honeyd προσομοιώνει τη συμπεριφορά της δικτυακής στοίβας των περισσότερων λειτουργικών συστημάτων. Η personality engine κάνει τη δικτυακή στοίβα των virtual hosts να μοιάζει αληθινή με το να πραγματοποιεί αλλαγές στις κεφαλίδες των πρωτοκόλλων κάθε εξερχόμενου πακέτου ώστε να μοιάζουν με τα χαρακτηριστικά του ρυθμισμένου λειτουργικού. Η βάση για αυτές τις αλλαγές είναι το fingerprint database του πιο γνωστού port scanner, του nmap [4]. Ένα από τα πρώτα βήματα για κάθε επιτιθέμενο είναι να κάνει ένα port scan στον host στον οποίο θα επιτεθεί, ώστε να δει τι υπηρεσίες τρέχει και ποιο λειτουργικό σύστημα. Είναι ιδιαίτερα σημαντικό οι honeyd hosts να ξεγελούν έναν επιτιθέμενο και να νομίζει ότι οι hosts είναι κανονικά συστήματα.

Ρύθμιση του honeyd

Το honeyd ρυθμίζεται από ένα κεντρικό αρχείο με λίγες εντολές και απλή σύνταξη. Οι υπηρεσίες που προσομοιώνονται βρίσκονται στον φάκελο scripts/ .

Οι εντολές είναι:

- create, δημιουργεί ένα template το οποίο ρυθμίζει το virtual host. Η λέξη default ως template είναι δεσμευμένη και ορίζει έναν host ο οποίος θα δίνεται σε οποιαδήποτε διεύθυνση στην οποία δεν έχει ρυθμιστεί κάποιο άλλο virtual host.
- set, δίνει την προσωπικότητα στο virtual host, δηλαδή το λειτουργικό σύστημα το οποίο προσομειώνει,πχ “Microsoft Windows NT 4.0 SP3”. Τα λειτουργικά που μπορούν να προσομειωθούν βρίσκονται στο αρχείο nmap.prints .Επίσης ορίζει την καθορισμένη συμπεριφορά των δικτυακών πρωτοκόλλων που ορίζουμε ως εξής: block κάνει drop όλα τα πακέτα, reset κλείνει όλες τις πόρτες και εμείς ορίζουμε ποιες θα είναι ανοικτές, open αφήνει όλες τις πόρτες ανοικτές.
- add, περιγράφει τις υπηρεσίες που θα είναι προσβάσιμες. Χρειάζεται να προσδιορίσουμε το πρωτόκολλο (tcp ,udp) της υπηρεσίας που θα τρέχει, την πόρτα και την εντολή που θα εκτελείται για την υπηρεσία (πχ scripts/web.sh). Επίσης υπάρχει η εντολή proxy με την οποία προωθούνται οι συνδέσεις σε κάποιον διαφορετικό κόμβο -πχ σε κάποιο άλλο honeypot ή στη διεύθυνση από την οποία προέρχεται η σύνδεση.
- bind , η οποία ορίζει ένα template στη διεύθυνση IP που προσδιορίζουμε.

Η ρύθμιση για το πως θα κατευθύνονται τα δεδομένα στους virtual hosts μας είναι ιδιαίτερης σημασίας.Τρία σενάρια είναι πιθανά:

- Δημιουργούμε τα route στον router μας που κατευθύνουν το μέρος του δικτύου που θέλουμε να δώσουμε στα virtual hosts, στο honeyd host.

- Κάνουμε χρήση του arpd -περιγράφεται αναλυτικά στο επόμενο κεφάλαιο. Το arpd βρίσκει τις διευθύνσεις που δεν χρησιμοποιούνται στο δίκτυο που του δίνουμε και οποιαδήποτε αίτηση για διεύθυνση ip στο δίκτυο αυτό περνάει στο honeyd host (arp spoofing). Αυτό γίνεται στην περίπτωση που έχουμε ένα ολόκληρο δίκτυο πχ C class το οποίο έχει ips που χρησιμοποιούνται αλλά και αδέσμευτες και θέλουμε να δώσουμε τις αδέσμευτες για παρακολούθηση, με δυναμική εύρεση αυτών. Όταν κάποιος επιχειρεί σύνδεση με κάποια ip του δικτύου που είναι αδέσμευτη, το honeyd δρομολογεί τη σύνδεση στο honeyd virtual host. Όταν κάνουμε προσομοίωση μιας τοπολογίας δικτύου δεν μπορεί να χρησιμοποιηθεί αυτή η μέθοδος. Επίσης αυτή η μέθοδος θα σταματήσει τυχόν DHCP daemon που τρέχει και ενδέχεται να προκαλέσει havoc στο δίκτυο.

- Με χρήση arp-proxy συσχετίζουμε ip διευθύνσεις που δεν έχουν δεσμευτεί με τη διεύθυνση MAC του honeyd host, στατικά όμως και όχι δυναμικά όπως το arpd. Αυτό βολεύει πολύ στην περίπτωση που έχουμε πχ μερικές ips στο δίκτυο που θέλουμε να τις δώσουμε για virtual honeypots. Αντί να χρησιμοποιούμε το arpd να παρακολουθεί το δίκτυο ,μόνοι μας "δανείζουμε " τη διεύθυνση MAC του honeyd μας σε αυτές. Η εντολή

arp -s "ip_διεύθυνση_virtual_host" "MAC_διεύθυνση_του_honeyd"

εκτελείται μια φορά και το πετυχαίνει αυτό. Τώρα όταν κάποιος επιχειρήσει σύνδεση σε μια από αυτές τις ips ,το honeyd θα απαντήσει αυτόματα με τη δική του MAC διεύθυνση, χωρίς την ανάγκη του arpd. Το μειονέκτημα αυτής της μεθόδου είναι οτι απαιτεί να έχουμε πρόσβαση στον router, γιατι το arp-proxy δουλεύει στον router.

Για παράδειγμα, η παρακάτω ρύθμιση δημιουργεί δυο virtual hosts, έναν Windows NT 4.0 virtual host με ip 10.0.0.51 και έναν OpenBSD 2.9-stable με ip 10.0.0.52, ενώ η διεύθυνση του honeyd είναι 10.0.0.1 .

Για να απαντάνε οι παραπάνω διευθύνσεις όταν δέχονται κίνηση προς αυτές πρέπει να τρέχει το arpd στο honeyd.Ο ρόλος του είναι να στέλνει spoofed απαντήσεις, εκ μέρους των virtual hosts που θέλουμε.

```
# ./arpd 10.0.0.51-10.0.0.52
```

Το arpd τώρα θα απαντήσει με τη διεύθυνση MAC του honeyd host για οποιαδήποτε αίτηση στις ip's 10.0.0.51 10.0.0.52. Η ρύθμιση γίνεται στο αρχείο honeyd.conf το οποίο είναι το αρχείο configuration για τους virtual hosts:

```
create windows

set windows personality "Windows NT 4.0 Server SP5-SP6"
```

```
add windows tcp port 80 “perl scripts/iis-0.95/iisemul18.pl”
add windows tcp port 139 open
add windows tcp port 135 open
set windows default tcp action reset
set windows default udp action reset
create relay
set relay personality "OpenBSD 2.9-stable"
add relay tcp port 25 "sh scripts/sendmail.sh $ipsrc $sport $ipdst $dport"
add relay tcp port 3128 "sh scripts/squid.sh $ipsrc $sport $ipdst $dport"
add relay tcp port 8080 "sh scripts/proxy.sh $ipsrc $sport $ipdst $dport"
set relay default tcp action block
set relay default udp action block
bind 10.0.0.51 windows
bind 10.0.0.52 relay
```

Δημιουργείται ο virtual host windows με λειτουργικό σύστημα Windows NT 4.0, τρέχει την υπηρεσία web, έχει ανοικτές τις πόρτες 135 και 139 και τις υπόλοιπες κλειστές. Αν κάποιος επιχειρήσει σύνδεση με την πόρτα 80, το honeypot θα ξεκινήσει το iisemul18.pl μέσω της perl -πρόκειται για emulator του IIS.

Η default συμπεριφορά του icmp είναι open, ώστε οι hosts να μπορούν να απαντάνε σε pings.

Επίσης δημιουργείται ο virtual host relay με λειτουργικό σύστημα OpenBSD 2.9-stable, ο οποίος τρέχει τις υπηρεσίες sendmail, squid, proxy στις πόρτες 25, 3128 και 8080, ενώ οι υπόλοιπες πόρτες είναι κλειστές.

Το honeyd ξεκινάει ως εξής:

```
# ./honeyd -p nmap.prints -f honeyd.conf 10.0.0.51-10.0.0.52
```

Με αυτό τον τρόπο περιμένει να εξυπηρετήσει αιτήσεις για τις ips 10.0.0.51 και 10.0.0.52 . Το -p nmap.prints δηλώνει πως η βάση με τα fingerprints βρίσκεται στο αρχείο nmap.prints Το -f honeyd.conf δηλώνει πως το honeyd βλέπει τη ρύθμιση του από το παραπάνω αρχείο. Το honeyd εμφανίζει ορισμένα μηνύματα στην οθόνη ότι ξεκίνησε ομαλά.

Παρατηρήσεις

- Η διεύθυνση του honeyd host δεν είναι απαραίτητο να είναι προσβάσιμη από έξω, οπότε θα μπορούσε να προστατευθεί μέσω του firewall. Έτσι ο honeyd host που είναι υπεύθυνος για τη δημιουργία των virtual hosts δεν μπορεί να δεχτεί επιθέσεις από το internet.
- Πέρα από το arp spoofing το οποίο καθιστά δυνατή την δρομολόγηση κίνησης, θα μπορούσε να δουλέψει και ο πρώτος ή ο τρίτος τρόπος δρομολόγησης των δεδομένων προς τα honeypots, που περιγράφονται παραπάνω.

- Η ρύθμιση αυτή είναι η πιο απλή που μπορεί να κάνει το honeyd. Πιο προχωρημένα και αληθοφανή σενάρια περιλαμβάνουν τη δημιουργία routers, επιπλέον ρυθμίσεις όπως uptime, droprate, uid, gid, δυναμικά templates τα οποία δίνουν δυνατότητα στο honeyd να αλλάξει τη δικτυακή συμπεριφορά ανάλογα με χαρακτηριστικά όπως time, source address, source os -passive fingerprinting-και διάφορα άλλα όπως latency, packet loss ...

logging

Το honeyd δημιουργεί logs από τις συνδέσεις που δέχτηκε τα οποία καταγράφουν τις προσπάθειες που έγιναν για σύνδεση αλλά και τις συνδέσεις που ολοκληρώθηκαν για όλα τα πρωτόκολλα, υπηρεσίες. Μπορεί να γίνει προβολή μέσω του stderr και του syslog, ή να αποθηκευτούν σε αρχείο. Επιπλέον, ιδιαίτερα χρήσιμες πληροφορίες θα πάρουμε αν το honeyd τρέχει σε συνδυασμό με κάποιο NIDS, όπως το πολύ γνωστό open source IDS snort.

Performance evaluation

Από πειράματα που έγιναν από το δημιουργό του honeyd , ένας υπολογιστής P3 1.1Ghz με δίκτυο 100Mbps μπορεί να εξυπηρετήσει πάνω από 2000 tcp συνδέσεις/sec .Επιτρέπεται δηλαδή η δημιουργία honeynet αποτελούμενο από χιλιάδες virtual honeypots -αν το δίκτυο μπορεί να διαθέσει φυσικά.

Εφαρμογές Honeyd

Το honeyd μπορεί να χρησιμοποιηθεί για τις εφαρμογές που ακολουθούν σε διαφορετικούς τομείς της ασφάλειας δικτύων.

- Εφαρμογή honeyd #1 : network decoys

Ένας επιτιθέμενος μπορεί να μπερδευτεί στις προσπάθειες του να συνδεθεί με τα virtual hosts που δημιουργεί το honeyd και να αποθαρρυνθεί από το να συνεχίσει τις προσπάθειες του για διείσδυση στο δίκτυο. Εφόσον δεν μπορεί να έχει κάποιο κέρδος από τα virtual hosts και δεν μπορεί να τα παραβιάσει, η όλη σύνδεση του αποτελεί χάσιμο χρόνο γι' αυτόν. Όπως και να' χει η προσπάθεια του θα καταγραφεί από το honeyd και θα υπάρχει ενημέρωση γύρω από την επίθεση.

- Εφαρμογή honeyd #2 : εργαλείο μάθησης

Το honeyd είναι ένα πολύ χρήσιμο open source εργαλείο για να πάρουμε μια εικόνα του τι συμβαίνει στο δίκτυο μας, από πλευράς επιθέσεων, να δούμε hosts από το δίκτυο μας οι

οποίοι είναι μολυσμένοι από worms και σε συνδυασμό με κάποιο ids να μελετήσουμε τις τεχνικές που χρησιμοποιούνται για την παραβίαση της ασφάλειας των συστημάτων. Επιτρέπει την εύκολη και γρήγορη δημιουργία δικτύων κάτι που μπορεί να χρησιμοποιηθεί για την πραγματοποίηση πειραμάτων.

- Εφαρμογή honeyd #3 : Honeyd vs worms

Μπορεί να χρησιμοποιηθεί στην έρευνα για την καταπολέμηση των worms [5], να εντοπίσει καινούργια worms ή ακόμα και να λάβει ενεργά μέτρα ενάντια στα μολυσμένα μηχανήματα. Μέσα σε μικρό χρονικό διάστημα ένα δίκτυο με honeyd virtual hosts θα συγκεντρώσει μεγάλη κίνηση από δραστηριότητα worms, η οποία αν μελετηθεί θα δώσει πληροφορίες για το ποια worms είναι ενεργά και για τη συμπεριφορά τους. Αν μάλιστα τρέχει και κάποιο ids ή network sniffer θα καταγράψει το payload του worm. Το πιο ενδιαφέρον πάντως σε αυτή την κατηγορία είναι ο καθαρισμό των μολυσμένων από worms hosts που επιχειρούν συνδέσεις με το honeyd -πχ στην περίπτωση worms όπως ο code red, nimda, msblaster κτλ που όταν μολύνουν έναν host μέσω αυτού επιχειρούν να συνδεθούν με ips που διαλέγουν με τυχαίο τρόπο και να προσπαθήσουν να τις μολύνουν-αν φυσικά αυτές τρέχουν τη μολυσμένη υπηρεσία και δεν έχει μπει το patch/update.

Στην περίπτωση αυτή ο μολυσμένος host που πλέον λειτουργεί σαν “ζόμπι” επιχειρεί σύνδεση με τυχαίες ips με σκοπό να μεταδωθεί το worm. Έτσι συνδέεται και με κάποιο virtual host, στο οποίο έχουμε δώσει οδηγίες όταν επιχειρείται σύνδεση στην πόρτα που μας ενδιαφέρει, να εκτελεί ένα script με το οποίο το κατευθύνουμε να τρέξει το exploit για το vulnerability που έχει ο host-ζόμπι και αφού αποκτήσει πρόσβαση σε αυτόν να εφαρμόσει το patch ή απλά να σβήσει τον ιο!

Το σενάριο αυτό δοκιμάστηκε με επιτυχία από ερευνητές ενάντια στον ιο msblaster.

Το σενάριο να γίνει κάποιο scan στο internet προς αναζήτηση ευαλωτων σε κάποια ευπάθεια hosts ,αλλά όχι για να βάλει κάποιος να επιτεθούν σε κάποιο στόχο, όπως πχ γίνεται μέχρι τώρα, αλλά αντίθετα για να patch-άρουν τα συστήματα αυτά είναι πιθανό, αλλά ηθικοί και νομικοί λόγοι εμποδίζουν την πραγματοποίηση ενός τέτοιου πειράματος.

Από την εντελώς αντίθετη πλευρά, είναι το εφιαλτικό σενάριο να χρησιμοποιηθούν χιλιάδες ή εκατομμύρια honeyd virtual hosts συνδεδεμένα σε δίκτυα ανταλλαγής αρχείων peer to peer, σαν hosts με ψεύτικα αρχεία προς ανταλλαγή ,τα οποία θα περιέχουν ιους -πχ σε αρχεία exe,jpg,mp3 [7]. Έχει αποδειχθεί οτι η RIAA, η MPAA και άλλες οργανώσεις για την προστασία των εταιρικών δικαιωμάτων των πολυεθνικών εταιρειών μουσικής και ταινιών παρακολουθούν και καταγράφουν την κίνηση τέτοιων δικτύων [8] και περιστασιακά μηνύουν απλούς χρήστες [9], “προσπαθώντας” με τον τρόπο αυτό να σταματήσουν την πειρατεία, η οποία όπως διαφαίνεται περιορίζει τις εισπράξεις των μικρών συγκροτημάτων, αλλά αντίθετα αυξάνει τα έσοδα των μεγάλων συγκροτημάτων και καλλιτεχνών .

- Εφαρμογή honeyd #4 : spam prevention

Το honeyd μπορεί να χρησιμοποιηθεί για να καταλάβουμε πως οι spammers λειτουργούν, καθώς επίσης και να αυτοματοποιηθεί η αναγνώριση καινούργιου spam, το οποίο και στέλνεται σε spam φίλτρα. Περισσότερα για την έρευνα πάνω στην καταπολέμηση του spam στο κεφάλαιο 7 “πολεμώντας το spam”.

ΣΗΜΕΙΩΣΕΙΣ -ΠΑΡΑΠΟΜΠΕΣ

[1] Το site του honeyd, www.honeyd.net

[2] A virtual honeypot framework (Provos, Usenix sec 04)

[3] Πληροφορίες για το πρωτόκολλο GRE RFC 1701, October 1994, Generic Routing Encapsulation (GRE)

[4] Το site για το γνωστότερο εργαλείο ασφάλειας δικτύων, το nmap network security scanner www.insecure.org

[5] Fighting internet worms with honeypots, oudot, securityfocus.com

[6] Simulating networks with honeyd (Chandran, Pakala)

[7] Towards evil honeypots(oudot,cansecwest 04)

[8] RIAA -the new superspy, http://www.xblock.com/articles/article_show.php?id=12

[9]RIAA Cracks Down On Internet2 File Sharing, http://yro.slashdot.org/article.pl?sid=05/04/12/1927210&tid=123&tid=141

[10] Honeypots against worms (oudot, black hat 03)

[11] wireless honeypot trickery (oudot, securityfocus.com)

[12] retaliation with honeypots (oudot, 5th hope)

[13] Honeypots (Spitzner, Addison Wesley)