Εισαγωγή στο Penetration Testing

+---

|K|a|r|a|g|i|a|n|n|i|s| |S|t|y|l|i|a|n|o|s| - |P|e|n|e|t|r|a|t|i|o|n| |T|e|s|t|i|n|g|

+---

IONIAN UNIVERSITY

- Μικρός Βοηθός - Short Manual -

Περιεχόμενα

#0x100 Εισαγωγή

Πριν ξεκινήσουμε είναι σημαντικό να κατανοήσουμε τις μεθοδολογικές προσεγγίσεις που αφορούν το Penetration Testing (Έλεγχος διείσδυσής). Η μεθοδολογία που ακολουθείται περιλαμβάνει βήματα τα οποία δεν είναι προκαθορισμένα και εξαρτώνται από το περιβάλλον και τις απαιτήσεις που θέτουμε. Δεν υπάρχουν προκαθορισμένες μεθοδολογίες και βήματα, ωστόσο υπάρχουν κάποια πρότυπα τα οποία είναι σημαντικό να τα γνωρίζουμε.

#0x110 Διαφορετικές προσεγγίσεις PenTesting:

Black: Καμία γνώση για την υποδομή.

Grey: Περιορισμένη γνώση της υποδομής.

White: Ο έλεγχος γίνεται σε συνεργασία με τους διαχειριστές του δοκιμαζόμενου δικτύου.

#0x120 Γιατί να επιλέξουμε τη διενέργεια penetration test?

1. Το “hacking” πλέον αποτελεί μια αυτόματη διαδικασία καθώς πολλά αυτόματα εργαλεία είναι διαθέσιμα online. Τέτοια εργαλεία δίνουν τη δυνατότητα ακόμη και σε αρχάριους, μη πεπειραμένους hackers να απειλούν σημαντικά τους οργανισμούς.

2. Η διενέργεια penetration test βοηθά την επιχείρηση στην εύρεση των ευπαθειών της προτού εκείνες γίνουν αντιληπτές από επιτιθέμενους.

Επιπλέον, μέσα από το pen-test γίνονται αντιληπτά προβλήματα των οποίων η ύπαρξη αγνοούταν.

3. Το penetration test προσφέρει μια ανεξάρτητη οπτική της αποτελεσματικότητας των διαδικασιών ασφάλειας ενός οργανισμού.

4. Συχνά penetration tests οδηγούν στην ανακάλυψη νέων απειλών και ευπαθειών, πριν αυτές προκαλέσουν ζημία στην επιχείρηση.

5. Η διενέργεια pen-tests παρέχει τη βάση για τη στρατηγική ασφάλειας που θα πρέπει να ακολουθήσει η εκάστοτε εταιρεία ανάλογα με τα αποτελέσματα του.

6. Παρέχει μετρήσιμα αποτελέσματα και αναφορά η οποία βοηθά στην λήψη μέτρων και διορθωτικών ενεργειών.

7. Ακόμα ένας λόγος για την επιλογή διενέργειας penetration test αποτελεί η κατηγοριοποίηση και προτεραιοποίηση των κινδύνων με βάση συγκεκριμένα κριτήρια ανά εταιρεία.

8. Με την ανάλυση της αποτελεσματικότητας των υπαρχόντων μέτρων ασφάλειας το penetration test δίνει τη δυνατότητα αιτιολόγησης μελλοντικών επενδύσεων.

9. Το penetration test αποτελεί μια οικονομική, αποδοτική και στοχευμένη προσέγγιση μείωσης των κινδύνων που διατρέχει η εταιρεία ή οργανισμός.

10. Επιπλέον λόγος επιλογής διενέργειας pen-test αποτελεί το γεγονός ότι συμμορφώνεται με τις απαιτήσεις διάφορων διεθνώς αναγνωρισμένων προτύπων όπως το ISO 27001, το PCI DSS κλπ.

11. Το penetration test επιτρέπει σε έναν οργανισμό να αποφύγει τις κυρώσεις που μπορεί να του επιφέρει μια μη συμμόρφωση, αφού γνωρίζει τις αδυναμίες του και έχει φροντίσει να λάβει τα απαραίτητα μέτρα για την έγκαιρη διόρθωσή τους.

12. Η διαδικασία των δοκιμών αυτών αποτελεί χρήσιμο εργαλείο στα χέρια της Διοίκησης του εκάστοτε οργανισμού καθώς δίνει μια γενική εικόνα σχετικά με το επίπεδο της ασφάλειας και το επίπεδο των κινδύνων στους οποίους αυτή εκτίθεται.

#0x130 Κατηγορίες PenTesting

1. Συστημάτων (System)
2. Δικτύων (Network)
3. Ασύρματου δικτύου (Wireless)
4. Εφαρμογών (Web App)
5. Εφαρμογών κΕφαρμογών (Web App)
6. Εφαρμογών κινητών συσκευών (Mobile App)
7. Κοινωνική Μηχανική (Social Engineering)
8. Φυσική πρόσβαση (Physical)

#0x140 Χρήσιμες έννοιες PenTesting:

- Απειλή (Threat): Ένα στοιχείο που μπορεί να προκαλέσει ζημιά στο πληροφοριακό σύστημα.
- Ευπάθεια (Vulnerability): Μια αδυναμία που μπορεί να χρησιμοποιήσει κάποιος ώστε να προκαλέσει ζημιά σε ένα πληροφοριακό σύστημα.
- Εκμετάλλευση (Exploit): Είναι η τεχνική ή ο κώδικας που μπορεί να χρησιμοποιήσει μια οντότητα ώστε να εκμεταλλευτεί μια αδυναμία ενός πληροφοριακού συστήματος με σκοπό να προκαλέσει ζημιά.
- Φορτίο (Payload): Είναι το σημείο εκείνο του κώδικα του exploit, το οποίο προσπαθεί ο επιτιθέμενος να να τρέξει στο μηχάνημα-στόχο

Για τις ανάγκες του εργαστηρίου θα αξιοποιήσουμε την μεθοδολογία PTES [PTES,2014], που αποτελεί μία προτυποποιημένη μεθοδολογία ελέγχου διείσδυσης. Το πρότυπο αυτό έχει ενημερωθεί και παραμαμετροποιηθεί πολλές φορές από το 2010.

Η μεθοδολογία PTES [PTES, 2014] αποτελεί όπως αναφέρει το όνομα της, μία μεθοδολογία για ελέγχους διείσδυσης. Το πρότυπο αναπτύσσεται από το 2010.

The Penetration Testing Execution Standard (PTES) - http://www.pentest-standard.org/index.php

Οι βασικές φάσεις της μεθόδου είναι:

1. Ενέργειες πριν τον έλεγχο (Pre-engagement Interactions). Αφορά όλη την προετοιμασία για το penetration testing. Κατά τη διάρκεια της συγκεκριμένης φάσης ο pentester έρχεται σε συνεννόηση με τον πελάτη ώστε να οριστεί επακριβώς το πεδίο δράσης του ελέγχου.
2. Συλλογή Πληροφοριών (Intelligence Gathering). Περιέχει όλες τις δραστηριότητες που πρέπει να γίνουν ώστε να αναγνωριστεί καλύτερα ο στόχος (πελάτης). Οι συνηθέστερες μέθοδοι σε αυτή τη φάση είναι η συλλογή πληροφοριών απο το διαδίκτυο (social media) με τη βοήθεια αυτοματοποιημένων εργαλείων, προσωπική ανάλυση στόχου επιφανειακά ή σε βάθος. Είναι πολύ σημαντικό στάδιο για τη συνέχεια του PenTesting καθώς ορίζει τις διαφορετικές μεθόδους επίθεσης που θα εκτελεστούν σε επόμενο στάδιο.

3. Μοντελοποίηση απειλών (Threat Modeling). Καταμέτρηση όλων των αγαθών του πληροφοριακού συστήματος (πολιτικές, διαδικασίες, μηχανήματα, άνθρωποι, …) ,ανάλυση και αξιολόγηση τους με αποτέλεσμα τον υπολογισμό του "κόστους" απώλειας τους.
4. Ανάλυση ευπαθειών (Vulnerability Analysis). Αποτελεί τη διαδικασία εντοπισμού τρωτών σημείων σε πληροφοριακά συστήματα και εφαρμογές.
5. Εκμετάλλευση (Exploitation). Μετά τον εντοπισμό των ευπαθειών, πραγματοποιείται η επίθεση στα τρωτά σημεία του πληροφοριακού συστήματος με σκοπό την παράκαμψη των τεχνικών ασφάλειας και την πρόσβαση σε αυτό.
6. Κινήσεις μετά την εκμετάλλευση (Post Exploitation). Αποτελεί το σύνολο των κινήσεων που πρέπει να γίνουν μετά την επιτυχής πρόσβαση στο δοκιμαζόμενο σύστημα. Τέτοιες ενέργειες μπορεί να είναι η επαύξηση δικαιωμάτων, η πρόσβαση σε άλλα συστήματα του δικτύου, η απόκτηση αρχείων του πληροφοριακού συστήματος, η τοποθέτηση backdoor, ο καθαρισμός ιχνών κ.α..
7. Αναφορά (Reporting). Αποτελεί την εκτενή αναφορά που πρέπει να παραδοθεί μετά το τέλος όλων των παραπάνω φάσεων του PenTesting. Πρέπει να περιέχει όλες τις ενέργειες που εγιναν κάτα τη δοκιμή του πληροφοριακού συστήματος, τις τεχνικές που ακολουθήθηκαν και τα αποτελέσματα που εξήχθησαν. Δηλαδή πρέπει να αναλυθει κάθε ένα απο τα παραπάνω βήματα.

Στο εργαστήριο θα επικεντρωθούμε στα εξής βήματα:

1. Συλλογή Πληροφοριών (Intelligence / Information Gathering)
2. Ανάλυση Τρωτοτήτων (Vulnerability Analysis)
3. Εκμετάλλευση (Exploitation)

Τέλος θα αναλυθούν CTF (Capture the Flag) Πλατφόρμες και διάφορες μεθοδολογίες που μπορούν να ακολουθηθούν για την περαιτέρω εκπαίδευση πάνω στην κυβερναασφάλεια (cybersecrurity). Στο Κεφάλαιο 0x200 θα αναλυθούν οι τεχνικές λεπτομέρειες που αφορούν την εγκατάσταση και παραμετροποίηση των λειτουργικών συστημάτων καθώς και των ιδιοτήτων του δικτύου (network properties.

#0x200 Τεχνικές Λεπτομέρειες

Πριν ξεκινήσουμε με τις τεχνικές είναι σημαντικό να περιγράψουμε το περιβάλλον (λειτουργικά συστήματα, δίκτυο) στο οποίο θα εργαστούμε. Θα αξιοποιήσουμε την διανομή Kali Linux που θα τρέχει σε ένα εικονικό σύστημα στα Windows μέσω του Virtual Box.

Το virtual box είναι ένα πρόγραμμα που αξιοποιείται για να χρησιμοποιούμε πολλαπλά λειτουργικά συστήματα σε ένα. Παρόμοια προγράμματα είναι το VmWare, το Hyper-V και το Parallels μεταξύ άλλων. Εν συντομία το Virtual Box είναι ακρετά εύχρηστο και ευέλικτο (high portability). Ωστόσο το VmWare παρέχει καλύτερες επιδόσεις (higher performance). Για τις ανάγκες του εργαστηρίου θα χρησιμοποιήσουμε το Virtual Box. Το Kali Linux όπως και διάφορα άλλα images παρέχονται σε .iso αρχεία τα οποία είναι εικονικοί δίσκοι. Επίσης μετά την εγκατάσταση των συστημάτων στο virtual box μας δίνεται η δυνατότητα να εξάγουμε το συγκεκριμένο σύστημα σε .vbox image και να το εκτελέσουμε σε οποιοδήποτε λειτουργικό σύστημα.

Συγκεκριμένα θα τρέχουμε Kali Linux (Live Edition) σε Virtual Box με ανοιχτά τα Windows. Αργότερα θα τρέξουμε .vbox images που μας δίνουν έτοιμα συστήματα που έχουν ευπάθειες (vulnerable systems) ή συστήματα που έχουν προκαθορισμένα υπηρεσίες όπως web services κλπ.

Όσον αφορά τις ιδιότητες του δικτύου είναι σημαντικό να βρισκόμαστε όλοι στο ίδιο υποδίκτυο (subnet).

#0x210 Virtual Box

Συγκεκριμένα για το virtual box, επιλέγουμε τα resources από τις ιδιότητες καθώς και δημιουργούμε ένα .vdi image που αναπαριστά τον εικονικό σκληρό δίσκο του συστήματος που στήνουμε.

Σημαντικό είναι να επιλέξουμε το εικονικό σύστημα να είναι στο ίδιο υποδίκτυο με τα windows αλλά και τα υπόλοιπα εικονικά συστήματα που θα τρέχουν στο virtual box. Επιλέγουμε File -> Preferences και έπειτα στην καρτέλα Network. Πατάμε προσθήκη (add nat network) και με διπλό κλίκ επιλέγουμε το nat network που δημιουργήσαμε. Δίνουμε το όνομα Lab1 και για CIDR

τοποθετούμε το υποδίκτυο που βρισκόμαστε (πχ. 192.168.6.0/24). Επιλέγουμε supports DHCP για να αποδώσει δυναμική ip σε οποιοδήποτε εικονικό λειτουργικό σύστημα βρίσκεται στο Lab1 και πατάμε ok.

#0x220 Kali Linux

Συγκεκριμένα για το virtual box, επιλέγουμε τα resources από τις ιδιότητες καθώς και δημιουργούμε ένα .vdi image που αναπαριστά τον εικονικό σκληρό δίσκο του συστήματος που στήνουμε.

Προκαθορισμένοι κωδικοί (default passwords username/password): root / toor

Σημαντικό είναι να επιλέξουμε το εικονικό σύστημα να είναι στο ίδιο υποδίκτυο με τα windows αλλά και τα υπόλοιπα εικονικά συστήματα που θα τρέχουν στο virtual box. Επιλέγουμε File -> Preferences και έπειτα στην καρτέλα Network. Πατάμε προσθήκη (add nat network) και με διπλό κλίκ επιλέγουμε το nat network που δημιουργήσαμε. Δίνουμε το όνομα Lab1 και για CIDR τοποθετούμε το υποδίκτυο που βρισκόμαστε (πχ. 192.168.6.0/24). Επιλέγουμε supports DHCP για να αποδώσει δυναμική ip σε οποιοδήποτε εικονικό λειτουργικό σύστημα βρίσκεται στο Lab1 και πατάμε ok.

#0x230 Linux Commands (Βασικές Εντολές)

mkdir directoryname: Δημιουργία φακέλου με όνομα "directoryname”

Pwd: Επιστρέφει το path που βρισκόμαστε

Grep: Αναζήτηση συμβολοσειράς

Ls: Προβολή αρχείων και φακέλων (ls -a για προβολή σε στήλες)

Sudo: Εκτέλεση εντολής ως superuser (πχ. sudo ls)

apt-get install packagename: Κατέβασμα και εγκατάσταση του πακέτου με όνομα packagename (πχ. sudo apt-get install gimp)

git clone "url“: Κατέβασμα ενός github repository στον τοπικό φάκελο (πχ. git clone https://github.com/azet/thc-tls-dos θα κατεβάσει όλα τα αρχεία του repository στον φάκελο thc-tls-dos)

cat filename: Προβολή δεδομένων ενός αρχείου

vi filename: Άνοιγμα αρχείου με τον file editor vi

strings filename: Αξιοπποιείται για να εξάγουμε τα στοιχεία από binary files

Ifconfig: Προβολή των ρυθμίσεων των lan interfaces (wlan included)

Ping: Pinging ip address or domain names

Traceroute: Προβολή των nodes που περνούν τα πακέτα μέχρι τον τελικό προορισμό τους

find / -name "name” : Αναζήτηση αρχείου "name" στο root folder

rm –rf filename : Διαγραφή του φακέλου ή αρχείου με όνομα “filename”

chmod : Αλλαγή δικαιωμάτων αρχείου

#0x300 Συλλογή Πληροφοριών (Intelligence Gathering)

Παθητική Συλλογή Πληροφοριών (Passive Information Gathering)

Ενεργητική Συλλογή Πληροφοριών (Active Information Gathering)

Σε αυτό το βήμα βρίσκονται οι ενέργειες που αποσκοπούν στην εύρεση πληροφοριών σχετικές με το στόχο. Η φάση αυτή διαχωρίζεται σε δύο λειτουργίες, την παθητική και την ενεργητική. Η Παθητική Συλλογή Πληροφοριών, αφορά τη συλλογή πληροφοριών που επιτυγχάνεται χωρίς τη δημιουργία ιχνών και γενικότερα χωρίς να γίνει αντιληπτή η αναζήτηση πληροφοριών από τον οργανισμό. Ειδικότερα, η παθητική συλλογή πληροφοριών αφορά την αναζήτηση σε καταλόγους και ευρετήρια με πληροφορίες σχετικές με τους υπάλληλους του οργανισμού, με τα περιουσιακά στοιχεία αυτού, την εύρεση πληροφοριών από φορολογικά αρχεία, ιστοσελίδων, κοινωνικών δικτύων, ομάδων ενημέρωσης, φυλλάδια και επαγγελματικές κάρτες.

Δεν αποτελεί έκπληξη για τη φάση αυτή, η αναζήτηση για επαγγελματικές συναντήσεις των υπαλλήλων, τις τοποθεσίες των γραφείων και διάφορες αγγελίες για δουλειά στον οργανισμό. Από τη παθητική συλλογή πληροφοριών δεν λείπει η ανίχνευση πακέτων δικτύου και η επεξεργασία αυτών για την ανακάλυψη ενεργών συσκευών. Η παθητική συλλογή μπορεί να ανακαλύψει μη κρυπτογραφημένους κωδικούς και ονόματα χρηστών καθώς και τα λειτουργικά συστήματα που χρησιμοποιούνται.

Η Ενεργητική Συλλογή Πληροφοριών ή και Χαρτογράφηση Δικτύου είναι η λειτουργία κατά την οποία συλλέγονται πληροφορίες σχετικές με το στόχο, όπως οι διευθύνσεις κεντρικών υπολογιστών, το λειτουργικό σύστημα που χρησιμοποιούν τα μηχανήματα και τις κρίσιμες υπηρεσίες που τρέχουν στις ανάλογες θύρες. Αυτή η διαδικασία επιτυγχάνεται "ενεργητικά" καθώς γίνεται χρήση εργαλείων που αποστέλλουν πακέτα και θεωρείται "θορυβώδης" έναντι της παθητικής συλλογής. Επίσης, συλλέγονται πληροφορίες για τις διαδικασίες που ακολουθούνται όπως είναι οι φυσικές τοποθεσίες μηχανημάτων, τα φυσικά μέσα προστασίας μέσω τεχνικών κοινωνικής μηχανικής ώστε να πραγματοποιηθεί ανάλυση στην επόμενη φάση.

#0x310 Παθητική Συλλογή Πληροφοριών (Passive Information Gathering)

Χρήσιμα Εργαλεία:

Wireshark: Το εργαλείο wireshark αποτελεί εργαλείο ανάλυσης πρωτοκόλλων στην κίνηση δικτύου.

Nmap - Zenmap: Στόχος του εργαλείου είναι να βοηθήσει το χρήστη να συγκεντρώσει όσο το δυνατόν περισσότερες πληροφορίες γίνεται ώστε να πραγματοποιήσει τις επόμενες φάσεις με σιγουριά. Το εργαλείο χρησιμοποιείται στη φάση της Συλλογής Πληροφοριών αλλά και τις Αναγνώρισης Τρωτοτήτων χάρη στη δυνατότητα του να χρησιμοποιεί διάφορες προσθήκες λογισμικού (extensions, plugins).

---

root@kali:~# nmap -sS 192.168.20.10-12 -oA booknmap

root@kali:~# nmap -sU 192.168.20.10-12 -oA bookudp

```
root@Kali:~# nmap -sS -p 3232 192.168.20.10
```

Maltego: Το maltego προσφέρει μία μοναδική προοπτική τόσο σχετικά με το δίκτυο όσο και με τις διάφορες οντότητες που βασίζονται στους πόρους του, όπως είναι η συγκέντρωση των πληροφοριών που δημοσιεύονται σε όλο το Διαδίκτυο. Αυτές οι πληροφορίες, για παράδειγμα, μπορεί να αφορούν την τρέχουσα διαμόρφωση του δρομολογητή που επικοινωνεί με το διαδίκτυο. Το maltego μπορεί να εντοπίσει και να απεικονίσει συνολικά αυτές τις πληροφορίες. Πιο συγκεκριμένα, μπορεί να χρησιμοποιηθεί για να προσδιορίσει τις σχέσεις και τους δεσμούς στην πραγματική ζωή μεταξύ ανθρώπων, ομάδων ανθρώπων, εταιρειών, οργανισμών, ιστοσελίδων, και πληροφορίες διαδικτύου όπως είναι οι περιοχές (domains), διευθύνσεις IP, συνεργασίες, έγγραφα και αρχεία.[Maltego,2014] Είναι σαφές από τη περιγραφή του εργαλείου ότι αυτό χρησιμοποιείται κατά τη φάση του Σχεδιασμού και της Προετοιμασίας αλλά και της Συλλογής Πληροφοριών (παθητική). Το Maltego της Paterva είναι ένα εργαλείο εξόρυξης δεδομένων που έχει σχεδιαστεί για να απεικονίζει συλλογή πληροφοριών.

ArpScan: Το arpscan αποτελεί εργαλείο σάρωσης (συχνά εμφανίζεται ως ARP sweep ή MAC scanner) και είναι ένας πολύ γρήγορος σαρωτής πακέτων ARP. Ο σκοπός του 61 εργαλείου είναι να υποδείξει κάθε ενεργό μηχάνημα (συσκευή) στο υποδίκτυο. Βέβαια, από τη στιγμή που το πρωτόκολλο ARP δεν έχει δυνατότητα δρομολόγησης, αυτό το είδος σάρωσης χρησιμοποιείται μόνο εντός υποδικτύου. Στα πλεονεκτήματα του εργαλείου συγκαταλέγεται η δυνατότητα του να ανακαλύπτει τις ενεργές συσκευές ακόμα και αν βρίσκονται πίσω από κάποιο τείχος προστασίας. Οι συσκευές δεν μπορούν να αρνηθούν την ύπαρξη τους στα ARP πακέτα, όπως μπορούν να κάνουν σε μία εντολή ping.[Arpscan,2014] Το εργαλείο αυτό χρησιμοποιείται κατά τη φάση της Συλλογής Πληροφοριών ή Αναγνώριση Δικτύου.

Social Engineer Tool SET: Το εργαλείο Social Engineer Tool είναι ειδικά σχεδιασμένο για να εκτελεί προηγμένες επιθέσεις εναντίον του ανθρώπινου στοιχείου. Το SET γρήγορα έγινε ένα αναπόσπαστο εργαλείο για τους επαγγελματίες ελεγκτές ασφάλειας. Οι επιθέσεις που είναι ενσωματωμένες στην εργαλειοθήκη του SET είναι σχεδιασμένες να στοχεύουν σε ένα πρόσωπο κάθε φορά ή και στον οργανισμό σαν ολότητα. Ο σκοπός του εργαλείου είναι η συλλογή πληροφοριών μέσω επιθέσεων κοινωνικής μηχανικής.[Social Engineer Tool, 2014] Το εργαλείο

συνήθως χρησιμοποιείται από κοινού με το εργαλείο Maltego. Είναι προφανές ότι η χρήση του εργαλείου συμβαίνει κατά τη φάση του Σχεδιασμού και της Συλλογής Πληροφοριών.

DnsDict6: Το συγκεκριμένο εργαλείο είναι ιδανικό για τη συγκέντρωση πληροφοριών σχετικές με το διακομιστή DNS. Το dnsdict6 μπορεί να απαριθμήσει διάφορες πληροφορίες, οι οποίες είναι μη ορατές στον απλό χρήστη. Το εργαλείο βρίσκεται όπως και πολλά άλλα στη σουίτα kali linux και σκοπός του είναι η ανεύρεση πληροφοριών όπως: πληροφορίες για υποτομείς(subdomains), τις διευθύνσεις IPv4 και IPv6, λεπτομέρειες σχετικές με srv αρχεία και λεπτομέρειες για τους διακομιστές.[DNSDict6,2014] Το εργαλείο χρησιμοποιείται κατά τη φάση της Αναγνώρισης Δικτύου.

DnsEnum: Το dnsenum δημιουργήθηκε για να πραγματοποιεί απαρίθμηση πληροφοριών σχετικές με το διακομιστή DNS και τους τομείς αυτού (domains). Ο σκοπός του εργαλείου είναι να συγκεντρώσει όσο το δυνατόν περισσότερες πληροφορίες για ένα τομέα. Το πρόγραμμα επί του παρόντος εκτελεί τις εξής λειτουργίες: απόκτηση ονόματος διακομιστή, απόκτηση διεύθυνσης ενεργών συσκευών (μηχανημάτων, κεντρικών υπολογιστ ών), απόκτηση του αρχείου MX, πραγματοποίηση axfr ερωτημάτων στους διακομιστές, απόκτηση επιπλέον ονομάτων μέσω της μηχανής αναζήτησης Google, υπολογισμός του εύρους της τάξης C στους τομείς των δικτύων και αντίστροφες αναζητήσεις (reverse lookups) στα εύρη των δικτύων.[DnsEnum,2014] Χρησιμοποιείται στη φάση της Αναγνώρισης Δικτύου.

DnsMap: Ο σκοπός του εργαλείου dnsmap είναι η ανακάλυψη τμημάτων (μπλοκ) από διευθύνσεις συσκευών στο δίκτυο. Το dnsmap κυρίως προορίζεται για να χρησιμοποιηθεί από τους ελεγκτές κατά τη διάρκεια της συλλογής πληροφοριών ή της απαρίθμησης σχετικά με την αξιολόγηση της ασφάλειας των υποδομών. Κατά το στάδιο αυτό, ο ελεγκτής θα προσπαθήσει να βρει τα εύρη των διευθύνσεων στο υποδίκτυο, τα ονόματα των τομέων, νούμερα τηλεφώνων. Επιπλέον, το εργαλείο έχει τη δυνατότητα να ανακαλύψει και τους υπο-τομείς από συγκεκριμένους τομείς (για παράδειγμα από το google.com είναι δυνατό να ανακαλύψει το mail.google.com, earth.google.com κλπ). Η ανακάλυψη των υποτομέων πραγματοποιείται με τη βοήθεια επιθέσεων ωμής βίας (brute force attack).[DNSMap,2014] Οι επιθέσεις αυτές είναι ιδιαίτερα χρήσιμες όταν τα άλλα είδη επιθέσεων δε λειτουργούν.

DnsTracer: Το dnstracer είναι ένα εργαλείο που χρησιμοποιείται στη φάση της συλλογής πληροφοριών για τον εξής λόγο. Είναι ικανό να καθορίσει από που ένας συγκεκριμένος διακομιστής DNS παίρνει τις πληροφορίες του και να ακολουθήσει την αλυσίδα των διακομιστών DNS πίσω σε εκείνους που γνωρίζουν τις 63 πληροφορίες.[DNSTracer,2014] Το εργαλείο βρίσκεται στη σουίτα εργαλείων του kali linux.

Fierce: Ο στόχος του εργαλείου είναι να συγκεντρώσει πληροφορίες σχετικές με το διακομιστή DNS. Χρησιμοποιείται ιδιαίτερα σε περιπτώσεις τέτοιες που οι διευθύνσεις του οργανισμού δεν είναι συνεχόμενες. Μία από τις βασικές λειτουργίες του εργαλείου είναι η δημιουργία DNS ερωτημάτων με σκοπό την εύρεση των διακομιστών του στόχου. Το εργαλείο αφού βρει το διακομιστή, μπορεί να το χρησιμοποιήσει και να διαγράψει τα αρχεία SOA του κάτω υπό το πρίσμα ότι ο διακομιστής μπορεί να μην έχει σωστές ρυθμίσεις. Αν αυτό αποτύχει, το εργαλείο χρησιμοποιεί μέσω επίθεσης ωμής βίας (brute force attack) να μαντέψει ονόματα τα οποία εμφανίζονται συχνά σε εταιρείες και οργανισμούς. Στη συνέχεια, αν το εργαλείο βρει κάτι σε κάποια IP διεύθυνση, θα σαρώσει πάνω και κάτω από αυτή τη διεύθυνση σε ένα προκαθορισμένο εύρος χρησιμοποιώντας αντίστροφη αναζήτηση. Αν βρει κάτι στη δευτερεύουσα αναζήτηση, θα επιχειρήσει ξανά αναζήτηση στο προκαθορισμένο εύρος γύρω από αυτήν. Η λειτουργία αυτή μπορεί να παρουσιάζει μία καθυστέρηση αλλά όσο μεγαλύτερη η καθυστέρηση τόσο μεγαλύτερη η έκταση των αποτελεσμάτων.[Fierce,2014] Το εργαλείο χρησιμοποιείται κατά τη φάση της Αναγνώρισης Δικτύου.

TcpFlow: Το εργαλείο αυτό καταγράφει τα δεδομένα που διαβιβάζονται στο πλαίσιο των TCP συνδέσεων, και αποθηκεύει τα δεδομένα κατά τρόπο τέτοιο που είναι κατάλληλος για την ανάλυση των πρωτοκόλλων ή τον εντοπισμό σφαλμάτων. Το tcpflow έχει την ικανότητα να παρουσιάζει μία περίληψη των πακέτων που ανταλάσσονται στην επικοινωνία. Επιπλέον, το tcpflow, ανακατασκευάζει τις πραγματικές ροές δεδομένων και αποθηκεύει κάθε ροή σε ξεχωριστό αρχείο για μετέπειτα ανάλυση. Αυτό συμβαίνει επειδή το tcpflow αντιλαμβάνεται τους αριθμούς ακολουθίας και έτσι μπορεί και ανακατασκευάζει σωστά τις ροές δεδομένων, ανεξάρτητα από αναμεταδόσεις ή 64 παραδόσεις πακέτων με λάθος σειρά.[TcpFlow,2014] Το εργαλείο χρησιμοποιείται κατά τη φάση της Αναγνώρισης Δικτύου.

Creepy: Το Creepy είναι μία απλή εφαρμογή που λαμβάνει τα ονόματα των χρηστών στο Twitter και το Flickr και εξάγει δεδομένα geolocation που περιέχουν πληροφορίες που έχουν δημοσιεύσει αυτοί οι χρήστες σε αυτές τις υπηρεσίες. Το ποσό της πληροφορίας που δημοσιεύεται με την ανάρτηση μίας φωτογραφίας με γεωγραφικό προσδιορισμό σε υπηρεσίες όπως το foursquare είναι τεράστιο. Το creepy επιτρέπει στο χρήστη να δει τις τοποθεσίες που άλλοι χρήστες με δημοσιευμένες φωτογραφίες ή πληροφορίες έχουν βρεθεί και να δημιουργήσει μία αλυσίδα με αυτές τις τοποθεσίες. Το εργαλείο είναι εξαιρετικά εύκολο στη χρήση. Ο χρήστης πληκτρολογεί το όνομα χρήστη στο Twitter η το Flickr και αφήνει το εργαλείο να αναζητήσει και να εξάγει αποτελέσματα. Μόλις η αναζήτηση ολοκληρωθεί, ο χρήστης θα λάβει ένα χάρτη με όλες τις τοποθεσίες που το εργαλείο. Εκτός από το χάρτη, τα αποτελέσματα συνθέτονται από μία λίστα με τις τοποθεσίες σε χρονολογική σειρά. Σε αυτή τη λίστα, ο χρήστης του Creepy μπορεί να κάνει δεξί κλικ και να περιηγηθεί μέσω του λογισμικού Google Maps στην ακριβή τοποθεσία.[Creepy,2014] Το εργαλείο χρησιμοποιείται κατά τη φάση της Συλλογής Πληροφοριών.

Metagoofil: Το metagoofil είναι ένα εργαλείο που χρησιμοποιείται κατά τη συλλογή πληροφοριών. Πιο συγκεκριμένα, το εργαλείο χρησιμοποιείται για την εξαγωγή πληροφοριών από δημόσια έγγραφα (pdf, doc, xls, ppt) που ανήκουν σε μία εταιρεία στόχο. Αρχικά, το εργαλείο εκτελεί μία αναζήτηση στη μηχανή αναζήτησης Google, για να εντοπίσει και να κατεβάσει τα έγγραφα στο τοπικό δίσκο και στη συνέχεια, θα εξάγει μεταδεδομένα, με διαφορετικές βιβλιοθήκες, όπως HACHOIR, PdfMiner και άλλες. Τέλος, θα συγκεντρώσει τα αποτελέσματα σε μία αναφορά, με τα ονόματα, τις εκδόσεις του λογισμικού και των διακομιστών ή ακόμα και ονόματα μηχανημάτων για να βοηθήσει τους ελεγκτές μετέπειτα στις επόμενες φάσεις.

```
metagoofil -d kali.org -t pdf -l 100 -n 25 -o kalipdf -f kalipdf.html
```

Theharvester: Το συγκεκριμένο εργαλείο έχει σαν στόχο να βοηθήσει τον ελεγκτή στα αρχικά στάδια του ελέγχου διείσδυσης να κατανοήσει το ηλεκτρονικό αποτύπωμα του (πελάτη) στόχου στο διαδίκτυο. Το εργαλείο είναι χρήσιμο στην οπτικοποίηση των πληροφοριών που υπάρχει στο διαδίκτυο για έναν οργανισμό και ενδεχομένως αυτές οι πληροφορίες να μπορούν να χρησιμοποιηθούν κακόβουλα.[theharvester, 2014] Ανήκει και αυτό όπως και τα προηγούμενα εργαλεία στη φάση της Συλλογής Πληροφοριών. Οι εξωτερικές δοκιμές διείσδυσης συχνά εντοπίζουν λιγότερες υπηρεσίες που είναι εκτεθειμένες από ότι οι εσωτερικές δοκιμές διείσδυσης.

Ένας εξαιρετικός τρόπος για να βρείτε τα ονόματα χρήστη είναι να αναζητήσετε διευθύνσεις ηλεκτρονικού ταχυδρομείου στο Ιντερνετ (από υπαλλήλους κλπ). Ενδέχεται να εκπλαγείτε να βρείτε εταιρικές διευθύνσεις ηλεκτρονικού ταχυδρομείου οι οποίες δημοσιεύονται δημόσια στις πληροφορίες επικοινωνίας των γονέων-εκπαιδευτικών, στις αθλητικές ομάδες και φυσικά, τα κοινωνικά μέσα. Το TheHarvester μπορεί να αυτοματοποιήσει την αναζήτηση στο Google, το Bing, το PGP, το LinkedIn και άλλα για την αναζήτηση email.

---

root@kali:~# Theharvester –d examplesite.com –l 500 –b searchengine

---

Twofi: Το όνομα του εργαλείου twofi προέρχεται από τις λέξεις Twitter Words Of Interest και όπως φαίνεται από το όνομα του επιχειρεί αναζητήσεις μέσω Twitter για λέξεις με ιδιαίτερο ενδιαφέρον. Πιο συγκεκριμένα, χρησιμοποιεί την υπηρεσία κοινωνικής δικτύωσης Twitter για να δημιουργήσει λίστες βασισμένες σε αναζητήσεις πάνω σε ένα χρήστη, εντοπίζοντας λέξεις κλειδιά. Το αποτέλεσμα της αναζήτησης αυτής είναι μία λίστα από λέξεις-κλειδιά στοιχισμένες σε φθίνουσα σειρά και ακολουθούμενες με τη συχνότητα εμφάνισης της λέξης. Στόχος του εργαλείου είναι να συλλέξει και να οργανώσει τη δομή των πληροφοριών για ένα χρήστη και να τις προβάλλει με τρόπο κατανοητό.[twofi, 2014] Το εργαλείο χρησιμοποιείται κατά τη φάση της Συλλογής Πληροφοριών

Dmitry: Το εργαλείο αυτό παίρνει το όνομα του από τα αρχικά των λέξεων Deepmagic Information Gathering Tool. Χρησιμοποιείται όπως φανερώνει και το όνομα του στη φάση της Συλλογής Πληροφοριών και έχει τη δυνατότητα να συλλέξει όσο το δυνατόν περισσότερες πληροφορίες για ένα κεντρικό υπολογιστή (host). Το εργαλείο είναι γραμμένο σε C, δίνοντας στο χρήστη μία γραμμή εντολών από την οποία εκτελεί 66 εντολές[Dmitry, 2014]. Η βασική λειτουργία του εργαλείου είναι οι αναζητήσεις whois, η εύρεση του χρόνου που μία υπηρεσία είναι ενεργή και να εκτελεί σαρωσεις TCP.

---

root@kali:~# Dmitry –w examplesite.com –n –s

root@kali:~# Golismero.py scan examplesite.com

NetDiscover: Το netdiscover είναι ένα εργαλείο ενεργητικής και παθητικής συλλογής πληροφοριών δικτύων, κυρίως προορισμένο για σάρωση ασύρματων δικτύων χωρίς τη παρουσία dhcp διακομιστή. Ο στόχος του εργαλείου είναι να βοηθήσει τον ελεγκτή να συλλέξει πληροφορίες σχετικές με τα δίκτυα στη φάση της Συλλογής Πληροφοριών. Το εργαλείο μπορεί να χρησιμοποιηθεί και σε δίκτυα με μεταγωγέα (switch) ή με κόμβο (hub). Είναι κατασκευασμένο πάνω στο libnet και libcap και μπορεί με χρήση παθητικής αναζήτησης να ανευρίσκει συνδεδεμένα μηχανήματα ή να τα αναζητήσει ενεργά με την αποστολή ARP πακέτων. Επιπλέον, το εργαλείο μπορεί να χρησιμοποιηθεί για την επιθεώρηση της κυκλοφορίας του arp δικτύου του χρήστη ή για να βρει διευθύνσεις στο δίκτυο χρησιμοποιώντας τη λειτουργία αυτόματης σάρωσης [NetDiscover, 2014].

Arping: Το arping είναι ένα εργαλείο λογισμικού που χρησιμοποιείται για να ανακαλύψει υπολογιστές (μηχανήματα) σε ένα δίκτυο υπολογιστών. Το λογισμικό ελέγχει αν μία διεύθυνση είναι ήδη σε χρήση στο τοπικό δίκτυο και μπορεί να λάβει επιπλέον πληροφορίες σχετικά με τον υπολογιστή που χρησιμοποιεί τη διεύθυνση. Το εργαλείο arping λειτουργεί με τρόπο που είναι ανάλογος με την εντολή ping, το οποίο ανιχνεύει υπολογιστές μέσω του πρωτοκόλλου ICMP. Η διαφορά εδώ είναι ότι ενώ το ICMP πρωτόκολλο έχει δυνατότητα δρομολόγησης καθώς λειτουργεί στο τρίτο επίπεδο της διασύνδεσης των συστημάτων OSI, το ARP δεν έχει αυτή τη δυνατότητα καθώς λειτουργεί στο δεύτερο επίπεδο. Έτσι, το εργαλείο λειτουργεί μόνο στο τοπικό δίκτυο. Υπάρχουν δύο βασικές υλοποιήσεις του εργαλείου, η μία είναι εκείνη που βρίσκεται κάτω από το πακέτο προγραμμάτων iputils και δεν έχει τη δυνατότητα ανεύρεσης MAC διευθύνσεων και εκείνη που είναι γραμμένη από τον Thomas Habets και έχει την 67 προηγούμενη δυνατότητα[arping, 2014]. Ο στόχος του εργαλείου είναι η αναγνώριση του δικτύου και η ανεύρεση πληροφοριών σχετικά με αυτό.

Fping: Το εργαλείο fping μοιάζει στη λειτουργία του με την εντολή ping το οποίο χρησιμοποιεί μηνύματα πρωτοκόλλου ICMP για να ανιχνεύσει μηχανήματα, μόνο που το fping διαφέρει στη δυνατότητα καθορισμού οποιουδήποτε αριθμού στόχων μέσω της γραμμής εντολών. Επιπλέον, δίνεται η δυνατότητα ο καθορισμός στόχων να γίνει μέσω καθορισμού αρχείου που τους περιέχει σε λίστα. Στην προεπιλεγμένη λειτουργία του, το εργαλείο θα στείλει ένα πακέτο και θα συνεχίσει να στείλει στον επόμενο ακολουθώντας τον αλγόριθμο round robin. Εάν κάποιος στόχος απαντήσει, τότε σημειώνεται και αφαιρείται από τη λίστα των στόχων προς έλεγχο. Εάν ένας στόχος δεν απαντήσει μέσα σε ένα προκαθορισμένο χρονικό διάστημα, τότε σημειώνεται σαν απρόσιτος.[fping, 2014] Το εργαλείο μοιάζει με το εργαλείο arping όσον αφορά στη βασική λειτουργία και μοιράζονται τον ίδιο στόχο, την αναγνώριση του δικτύου.

Hping: Το hping είναι ένας αναλυτής και εργαλείο συναρμολόγησης πακέτων TCP/IP. Παρέχει στο χρήστη μια γραμμή εντολών και όχι μία γραφική διεπαφή και είναι εμπνευσμένο από την εντολή ping των unix συστημάτων όπως και τα προηγούμενα εργαλεία. Το εργαλείο διαφέρει στο ότι δεν είναι μόνο σε θέση να στείλει ICMP μηνύματα αλλά και να υποστηρίξει επιπλέον τα πρωτόκολλα TCP, UDP, RAW-IP, παρέχει δυνατότητα ανίχνευσης διαδρομής πακέτων (traceroute) και δυνατότητα αποστολής αρχείων μεταξύ κρυφών καναλιών.[hping, 2014] Ο στόχος του εργαλείου είναι η αναγνώριση του δικτύου και η συλλογή πληροφοριών για αυτό.

Ncat: Το ncat είναι ένα εργαλείο που χρησιμοποιείται για ανάγνωση, γραφή, ανακατεύθυνση και κρυπτογράφηση των δεδομένων μέσα στο δίκτυο. Είναι άλλο ένα εργαλείο με γραμμή εντολών και όχι με γραφική διεπαφή όπως τα περισσότερα εργαλεία σε αυτές 68 τις φάσεις. Στόχος του εργαλείου είναι να λειτουργεί σαν ένας ελβετικός σουγιάς για τους ελεγκτές ασφάλειας ή τους διαχειριστές συστημάτων. Το ncat είναι κατάλληλο για διαδραστική χρήση ή για βοηθητικό εργαλείο ως προς άλλα εργαλεία. Το ncat λειτουργεί ως εξής: σαν ένας απλός TCP/UDP/SCTP/SSL εξυπηρετητής ο οποίος αλληλεπιδρά με διακομιστές διαδικτύου, telnet, εξυπηρετητής ηλεκτρονικής αλληλογραφίας, και άλλες υπηρεσίες του πρωτοκόλλου TCP/IP. Επίσης, το εργαλείο μπορεί να χρησιμοποιηθεί σαν δρομολογητής ανακατεύθυνσης ή μεσολάβησης της κυκλοφορίας των δεδομένων σε άλλες θύρες ή κεντρικούς υπολογιστές. Υποστηρίζει τεχνικές κρυπτογράφησης των πληροφοριών και τη μεταφορά τους στα πρωτόκολλα IPv4 και IPv6. Ακόμα, το ncat μπορεί να δράσει ως ενδιάμεσος σε σύνδεση δύο η περισσοτέρων εξυπηρετητών. Αυτό επιτρέπει πολλαπλά μηχανήματα που κρύβονται πίσω από NAT να επικοινωνούν μεταξύ τους.[ncat, 2014] Τέλος, το

εργαλείο μπορεί να εγκατασταθεί σε όλα τα γνωστά λειτουργικά συστήματα. Το εργαλείο χρησιμοποιείται κατά τη φάση της Συλλογής Πληροφοριών και της Αναγνώρισης Δικτύου.

Dnschef: Το dnschef είναι ένα ιδιαίτερα διαμορφώσιμο εργαλείο που λειτουργεί σαν ένας DNS διακομιστής μεσολάβησης που απευθύνεται σε ελεγκτές ασφάλειας και διαχειριστές συστημάτων. Ένας DNS διακομιστής μεσολάβησης ή αλλιώς και ψεύτικος DNS διακομιστής χρησιμοποιείται για την ανάλυση κίνησης τους δικτύου σε επίπεδο εφαρμογής. Για παράδειγμα, μπορεί να χρησιμοποιηθεί με σκοπό την αποστολή ψευδών αιτημάτων προς μία τρίτη ιστοσελίδα ώστε να οδηγήσει ένα μηχάνημα σε τερματισμό ή να υποκλέψει την κίνηση του. Η διαφορά του dnschef σε σχέση με άλλα παρόμοια εργαλεία, είναι ο μεγάλος βαθμός παραμετροποίησης του. Το γεγονός αυτό πηγάζει από το σκοπό τον οποίο υπηρετεί το εργαλείο αυτό, ο οποίος είναι η διενέργεια ενός ελέγχου διείσδυσης. Υποστηρίζεται σε πολλά λειτουργικά συστήματα, μπορεί να χρησιμοποιήσει λίστες αποκλεισμού, υποστηρίζει διάφορους τύπους αρχείων DNS, την αντιστοιχία διακομιστών με τη χρήση wildcards και τη ανακατεύθυνση μηνυμάτων σε διακομιστές που δεν έχουν αντιστοιχισθεί.[dnschef, 2014] Η χρήση του εργαλείου συνίσταται όταν δεν είναι δυνατή η αλλαγή του διακομιστή που χρησιμοποιεί μία εφαρμογή με άμεσο τρόπο.

Dsniff: Το dsniff δεν αποτελεί από μόνο του ένα εργαλείο αλλά μία συλλογή από εργαλεία για τον έλεγχο του δικτύου και των ελέγχων διείσδυσης. Τα εργαλεία που βρίσκονται στο dsniff είναι τα filesnarf, msgsnarf, urlsnarf, webspy. Αυτά χρησιμοποιούνται για την παθητική παρακολούθηση ενός δικτύου για ενδιαφέρονται στοιχεία, όπως είναι: κωδικοί πρόσβασης, διευθύνσεις email, αρχεία κ.ά. Επίσης, υπάρχουν τα arpspoof, dsnsspoof, macof που χρησιμοποιούνται για την υποκλοπή πληροφοριών που κανονικά δεν είναι διαθέσιμες στον επιτιθέμενο.[dsniff, 2014] Το εργαλείο χρησιμοποιείται κατά τη φάση της Συλλογής Πληροφοριών και Αναγνώρισης Δικτύου.

Ipscan: Σάρωση Ip στο δίκτυο και Port Scanning

Whois: Προβολή στοιχείων (Server name κλπ.). Όλοι οι καταχωρητές τομέα (registars διατηρούν αρχεία των τομέων που φιλοξενούν. Αυτά τα αρχεία περιέχουν πληροφορίες για τον ιδιοκτήτη, συμπεριλαμβανομένων των πληροφοριών επικοινωνίας.

---

root@kali:~# whois examplesite.com

Nslookup: Εμφάνιση των namservers. Οι διακομιστές DNS μεταφράζουν τη διεύθυνση URL που διαβάζεται από τον άνθρωπο σε διευθύνσεις IP.

---

root@kali:~# nslookup

> set type=mx

> bulbsecurity.com

Server: 75.75.75.75

Address: 75.75.75.75#53

Non-authoritative answer:

bulbsecurity.com mail exchanger = 40 ASPMX2.GOOGLEMAIL.com.

bulbsecurity.com mail exchanger = 20 ALT1.ASPMX.L.GOOGLE.com.

bulbsecurity.com mail exchanger = 50 ASPMX3.GOOGLEMAIL.com.

bulbsecurity.com mail exchanger = 30 ALT2.ASPMX.L.GOOGLE.com.

bulbsecurity.com mail exchanger = 10 ASPMX.L.GOOGLE.com.

Infoga: Συλλογή email λογαριασμών

Knockpy: Αναζήτηση subdomain (enumeration)

Recon-ng: Αυτό το εργαλείο μπορεί να είναι το πρώτο σας βήμα πριν ξεκινήσετε κάποιον έλεγχο σε έναν οργανισμό. Το recon-ng είναι πολύ καλό για αναζήτηση παθητικών πληροφοριών σχετικά με τον στόχο σας. Μπορεί να σας παρέχει πληροφορίες σχετικά με τα IP spaces, naming convention, τοποθεσίες, χρήστες, διευθύνσεις ηλεκτρονικού ταχυδρομείου, κωδικούς χρηστών αν υπήρξε κάποια διαρροή, και πολλά άλλα.

Για να εκτελέσετε το recon-ng

cd /η τοποθεσία που εγαταστήσατε το recon-ng/ && ./recon-ng

προσθέστε τα απαραίτητα στοιχεία workspaces add, add domains, add companies (Γενικές πληροφορίες για το σάρωμα). Επιλέξετε την μηχανή αναζήτησης που επιθυμείτε(google,bing) run

Το εργαλείο θα ψάξει για την μηχανή αναζήτησης για domain names, όπως φαίνετε στην πιο κάτω εικόνα.

Χρησιμοποιώντας ένα άλλο module μπορείτε να ανακαλύψετε subdomains
/domains-hosts/brute_hosts

Ο εκάστοτε χρήστης μπορεί να εκτελέσει πολλά modules π.χ. να αντιστοιχήσει διευθύνσεις IP με πραγματικές τοποθεσίες να αντιστοιχήσει domains με IPs και αντίστροφακ.ο.κ., τέλος το recon του δίνει την δυνατότητα να μαζέψει όλες τις πληροφορίες σε μια τελική αναφορά. Εκτελώντας την ποιο κάτω εντολή.

Usereporting/html
firefox /root/.recon-ng/workspaces/unipi/results.html

Discover Scripts: Πρόκειται για ένα εργαλείο πολύ εύκολο στην χρήση του και η ποσότητα των πληροφοριών που επιστρέφει είναι τεράστια. Το Discover εκτελεί μια παθητική σάρωση recon, και θα χρησιμοποιήσει ένα μεγάλο αριθμό άλλων εργαλείων όπως: dnsrecon, goofile, whois, googmail και πολλά άλλα. Για να τρέξετε το Discover εκτελέστε:

cd /η τοποθεσία που εγαταστήσατε το discover/ && ./discover.sh
Επιλέξτε 1 για σάρωση recon
Επιλέξτε 1 για παθητική σάρωση
Συμπληρώστε το όνομα του οργανισμού

Δώστε το domain του.
Εκτελέστε /root/data/το domain που δώσατε/index.html

SpiderFoot: Ένα τελευταίο εργαλείο που αξίζει αναφοράς είναι το SpiderFoot. Πρόκειται για ένα γρήγορο και εύχρηστο εργαλείο, που εκτελεί όπως και τα πιο πάνω πολλές σαρώσεις recon και επιστρέφει ένα μεγάλο αριθμό πληροφοριών. Για να χρησιμοποιήσετε το εργαλείο

cd /η τοποθεσία που εγαταστήσατε το SpiderFood/ spiderfoot-*/ && python sf.py
Ανοίξτε των περιηγητή στην σελίδα http://127.0.0.1:5001

Όπως, γνωρίζετε κάθε εργαλείο λειτουργεί διαφορετικά, και δεν είναι λίγες οι φορές που το ένα θα βρει διαφορετικές πληροφορίες από το άλλο, για αυτόν τον λόγο καλό είναι ένας ελεγκτής να μην περιορίζεται μόνο σε ένα σαρωτή OSINT. Με τα τρία εργαλεία που παρουσιάστηκαν πλέον έχουμε αρκετές πληροφορίες για τον οργανισμό. Αυτά τα δεδομένα θα είναι πολύτιμα κατά την διάρκεια του ελέγχου, οπότε βεβαιωθείτε ότι έχετε εξετάσει όλα τα δεδομένα επιμελώς