Εργαστήριο Δικτύων
Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

Ερωτήσεις κατανόησης και Εργασία για το μάθημα:
Σύγχρονες Εφαρμογές Ασφάλειας Δικτύων
Επιμέλεια/Προετοιμασία Άσκησης: **Απόστολος Κονταρίνης (*up1059565@upnet.gr*)**

Η εργασία αυτή είναι συνέχεια της εργασίας "DNS κακόβουλες επιθέσεις τύπου hijacking/pharming" και αφορά φοιτητές με περισσότερες γνώσεις στην δημιουργία εικονικών μηχανών και χρήση Linux. Η εργασία αφορά την υλοποίηση τριών εικονικών μηχανών και την εκτέλεση σεναρίων DNS cache poising. Αναλυτικές οδηγίες ακολουθούν.

Λογισμικό: VirtualBox. Χρήση Τριών Virtual Machines.

- User machine (Ubuntu ή Debian)
  - Ελάχιστα specs: 1 CPU, 512MB RAM
- DNS machine (Ubuntu ή Debian)
  - Ελάχιστα specs: 1 CPU, 512MB RAM
- Attacker machine (Ubuntu ή Debian)
  - Ελάχιστα specs: 1 CPU, 512MB RAM

(Εξαίρεση αν το host λειτουργικό σύστημα είναι είτε Debian είτε Ubuntu μπορεί να χρησιμοποιηθεί αντί για μίας εικονικής μηχανής).

Links για έτοιμες εικονικές μηχανές :
Debian: https://www.linuxvmimages.com/images/debian-10/P
Ubuntu: https://www.linuxvmimages.com/images/ubuntu-1804/
Μπορούν να εγκατασταθούν εύκολα με λειτουργία Import στο VirtualBox:

Βοηθητικό βίντεο:
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj77ajKgZTtAhUP2SoKHYZSDokQwqsBMAB6BAgSEAM&url=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3D93lM4OLyytE&usg=AOvVaw23AvxOmpQmhNBlNKWTtTHv

Στήσιμο Εργαστηρίου:

- Κάνουμε import 3 εικονικές μηχανές
- Στις ρυθμίσεις της κάθε εικονικές μηχανής στην κατηγορία Network επιλέγουμε Bridged Connection και όνομα το όνομα της κάρτας δικτύου του Host μηχανήματος
- Εσωτερικά στις εικονικές μηχανές στις ρυθμίσεις δικτύου τους κάνουμε set τις εξής IPs:
  - User machine: 192.168.x.100
  - DNS machine: 192.168.x.10
  - Attacker machine: 192.168.x.200

Το x εξαρτάται από την διεύθυνση του router του καθενός κάποια είναι 192.168.0, 192.168.1, 192.168.2 Διαλέγουμε το κατάλληλο

- Στην εικονική μηχανή DNS εκτελούμε τα παρακάτω βήματα:

- ***sudo apt-get install bind9***

Παραμετροποιούμε το DNS server εκτελώντας τα παρακάτω βήματα:

- στο αρχείο /etc/bind/named.conf.option προσθέτουμε:

```
options {
dump-file "/var/cache/bind/dump.db";
};
```

- στο αρχείο /etc/bind/named.conf προσθέτουμε:

```
zone "example.com" {
type master;
file "/var/cache/bind/example.com.db";
};
zone "0.168.192.in-addr.arpa" {
type master;
file "/var/cache/bind/192.168.0";
};
```

- Στον φάκελο /var/cache/bind/ δημιουργούμε αρχείο κειμένου με όνομα example.com.db και περιεχόμενα:

```
$TTL 3D
@ IN SOA ns.example.com. admin.example.com. (
2008111001 ;serial, today's date + today's serial number
8H ;refresh, seconds
2H ;retry, seconds
4W ;expire, seconds
1D) ;minimum, seconds
@ IN NS ns.example.com. ;Address of name server
@ IN MX 10 mail.example.com. ;Primary Mail Exchanger
www IN A 192.168.0.101 ;Address of www.example.com
mail IN A 192.168.0.102 ;Address of mail.example.com
ns IN A 192.168.0.10 ;Address of ns.example.com
*.example.com. IN A 192.168.0.100 ;Address for other URL in
;example.com. domain
```

- Στον φάκελο /var/cache/bind/ δημιουργούμε αρχείο κειμένου με όνομα 192.168.0 και περιεχόμενα:

```
$TTL 3D
@ IN SOA ns.example.com. admin.example.com. (
2008111001
8H
2H
4W
1D)
@ IN NS ns.example.com.
101 IN PTR www.example.com.
102 IN PTR mail.example.com.
10 IN PTR ns.example.com.
```

- Επανακινούμε το service: sudo service bind9 restart

- **Στην εικονική μηχανή User εκτελούμε τα παρακάτω βήματα:**
  - Στον φάκελο /etc/resolv.conf προσθέτουμε
    nameserver 192.168.0.10
  - Στις ρυθμίσεις δικτύου εκεί που ορίσαμε το IP προσθέτουμε ως DNS το IP της εικονικής μηχανής DNS δηλαδή 192.168.x.10
  - Restart machine
- **Στην εικονική μηχανή Attacker εκτελούμε τα παρακάτω βήματα:**:
  - Εγκαθιστούμε τα εργαλεία: Netwag, Netwox
    - sudo apt-get install netwag
    - sudo apt-get install netwox

Για τον έλεγχο ότι το set up έγινε σωστά, (ενώ οι εικονικές μηχανές User και DNS τρέχουν), εκτελούμε την εντολή **dig www.example.com**
και το αποτέλεσμα θα πρέπει να είναι σαν και το ακόλουθο:

<<>> DiG 9.5.0b2 <<>> www.example.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27136
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; QUESTION SECTION:
;www.example.com. IN A
;; ANSWER SECTION:
www.example.com. 259200 IN A 192.168.0.101
;; AUTHORITY SECTION:
example.com. 259200 IN NS ns.example.com.
;; ADDITIONAL SECTION:
ns.example.com. 259200 IN A 192.168.0.10
;; Query time: 80 msec
;; SERVER: 192.168.0.10#53(192.168.0.10)
;; WHEN: Tue Nov 11 15:26:32 2008
;; MSG SIZE rcvd: 82

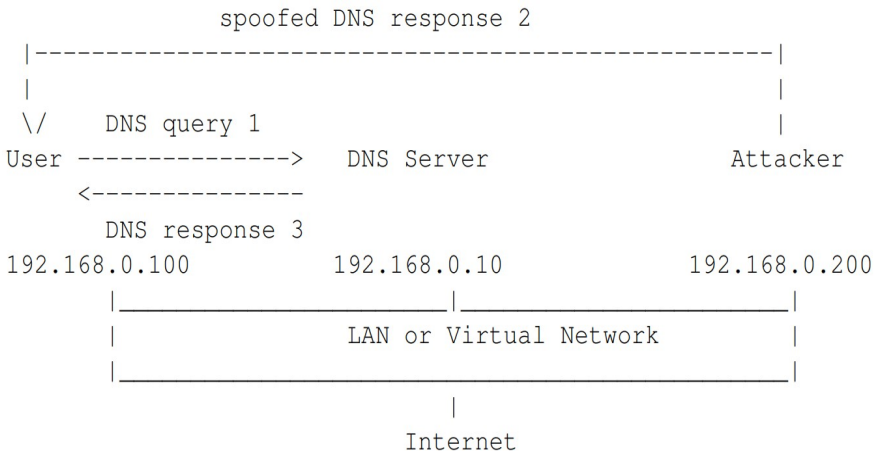
Ερωτήσεις:

1 Έστω ότι επιτιθέμενος έχει πρόσβαση στον υπολογιστή του θύματος (User machine). Να κάνετε modify το αρχείο HOSTS ώστε για την σελίδα www.example.com ο χρήστης να γίνεται redirect σε προεπιλεγμένη ip (διαλέξτε μια τυχαία αλλά πραγματική). Μπορείτε να το δοκιμάσετε αν ήταν επιτυχημένο, με την εντολή ping στην σελίδα www.example.com , το αποτέλεσμα της οποίας (της εντολής) θα είναι η προεπιλεγμένη ip

2 Αναιρέστε τις αλλαγές στο αρχείο HOSTS στο User machine. Σε αυτό το ερώτημα καλείστε να πραγματοποιήσετε DNS spoofing με την εφαρμογή netwox (***sudo apt-get install netwox)*** κάνοντας χρήση του ***εργαλείου 105*** στο Attacker machine. Θα πρέπει όταν ο χρήστης

πραγματοποιεί αίτημα για την σελίδα www.example.com να γίνεται redirect σε άλλη IP διεύθυνση που θα έχει επιλεχθεί από τον Attacker. Ο έλεγχος θα γίνει με ping από τον User στην σελίδα www.example.com.

Οπτική απεικόνιση επίθεσης:



3 Αδειάζουμε την cache του DNS machine με την εντολή $ sudo rndc flush. Σε αυτή την επίθεση αντί να δώσουμε ψευδή πληροφορία στο χρήστη για την πραγματική διεύθυνση του ισοτόπου που ζήτησε, πραγματοποιούμε την ίδια διαδικασία για τον DNS. Έτσι όταν ο χρήστης ζητήσει την σελίδα www.example.com ο DNS θα του δώσει λάθος πληροφορία για όσο χρόνο αυτή η λάθος πληροφορία μένει στην cache του DNS. Θα χρειαστείτε το ίδιο εργαλείο του Netwox και αυτή την φορά φροντίστε το TTL της απάντησης που θα δώσει το Attacker machine να είναι μεγάλο ώστε να μείνει στην cache του DNS περισσότερο χρόνο. Ο έλεγχος θα γίνει με ping από τον User στην σελίδα www.example.com.
Οπτική απεικόνιση επίθεσης: