

Σύγχρονες Εφαρμογές Ασφάλειας Δικτύων

Μπουρλάκης Γεώργιος

1054321

DNS κακόβουλες επιθέσεις τύπου hijacking/pharming

1) Ακολουθώντας ακριβώς τα απαραίτητα βήματα για δημιουργία του debian VM στη πλατφόρμα okeanos απέκτησα την public IP: [REDACTED]

Παρακάτω φαίνονται η αλλαγή δικαιωμάτων στο αρχείο id_rsa και η ssh σύνδεση χρησιμοποιώντας το private key χωρίς να ζητηθεί κάποιος κωδικός.

```
root@debian:/home/george# cd .ssh
root@debian:/home/george/.ssh# ls
id_rsa
root@debian:/home/george/.ssh# chmod 000 id_rsa
root@debian:/home/george/.ssh#
root@debian:/home/george/.ssh# ssh -i /home/george/.ssh/id_rsa debian@[REDACTED]
The authenticity of host '[REDACTED]' can't be established.
ECDSA key fingerprint is SHA256:0SyBIW803Y3Yzx84Sviy519w6WP0ukynurzk7fKj904.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[REDACTED]' (ECDSA) to the list of known hosts.
Linux snf-879210 4.9.0-5-amd64 #1 SMP Debian 4.9.65-3+deb9u2 (2018-01-04) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
debian@snf-879210:~$
```

Στην συνέχεια φαίνεται η διαδικασία προσθήκης κωδικού στο χρήστη root.

```
debian@snf-879210:~$ sudo -i
root@snf-879210:~# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@snf-879210:~#
root@snf-879210:~# exit
logout
debian@snf-879210:~$
debian@snf-879210:~$ su
Password:
root@snf-879210:/home/debian#
```

2) Οι εντολές με sudo από το debian είναι:

- sudo iptables -A INPUT -p all -m state --state ESTABLISHED,RELATED -j ACCEPT
- sudo iptables -A INPUT -p tcp --destination-port 22 -s 150.140.0.0/16 -j ACCEPT
- sudo iptables -A INPUT -p tcp -s 192.168.1.0/24 --dport 22 -j ACCEPT
- sudo iptables -A INPUT -p udp --dport 53 -j ACCEPT
- sudo iptables -A INPUT -p tcp -s localhost -j ACCEPT
- sudo iptables -P INPUT DROP
- sudo iptables -P FORWARD DROP
- sudo iptables -P OUTPUT ACCEPT

```
root@snf-879210:/home/debian# sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source                destination            state
ACCEPT     all  --  anywhere              anywhere               state RELATED,ESTABLISHED
ACCEPT     tcp  --  150.140.0.0/16        anywhere               tcp dpt:ssh
ACCEPT     tcp  --  192.168.1.0/24        anywhere               tcp dpt:ssh
ACCEPT     udp  --  anywhere              anywhere               udp dpt:domain
ACCEPT     tcp  --  localhost             anywhere

Chain FORWARD (policy DROP)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@snf-879210:/home/debian#
```

Με την εντολή: `sudo iptables-restore < /etc/iptables/rules.v4` επαναφέρονται τα iptables που έχουμε φτιάξει.

Η εγκατάσταση του fail2ban έγινε κανονικά και δουλεύει όπως φαίνεται παρακάτω.

```
root@snf-879210:/etc/fail2ban# systemctl start fail2ban; systemctl status fail2ban -l
● fail2ban.service - Fail2Ban Service
   Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2020-11-28 17:55:39 UTC; 4min 58s ago
     Docs: man:fail2ban(1)
   Main PID: 1221 (fail2ban-server)
   CGroup: /system.slice/fail2ban.service
           └─1221 /usr/bin/python3 /usr/bin/fail2ban-server -s /var/run/fail2ban/fail2ban.sock -p /var/run/fail2ban/fail2ban.pid -x -b

Nov 28 17:55:38 snf-879210 systemd[1]: Starting Fail2Ban Service...
Nov 28 17:55:38 snf-879210 fail2ban-client[1217]: 2020-11-28 17:55:38,639 fail2ban.server [1219]: INFO Starting Fail2ban v0.9.6
Nov 28 17:55:38 snf-879210 fail2ban-client[1217]: 2020-11-28 17:55:38,640 fail2ban.server [1219]: INFO Starting in daemon mode
Nov 28 17:55:39 snf-879210 systemd[1]: Started Fail2Ban Service.
root@snf-879210:/etc/fail2ban#
```

3) Υλοποίηση DNS εξυπηρέτη

Κάνοντας τις κατάλληλες τροποποιήσεις ώστε να έχουμε σαν DNS server το vm στο okeanos και ενεργοποιώντας τις καταγραφές των queries με την εντολή:

```
rndc querylog
```

καταγράφονται όλα τα domains που πληκτρολογούμε από τον προσωπικό υπολογιστή και καταγράφεται επίσης η public ip που έχουμε εκτός LAN, η οποία είναι [REDACTED] όπως φαίνεται παρακάτω.

Your Public IPv4 Address Is: [REDACTED]

Παρακάτω φαίνονται τα domains που πληκτρολογούνται από τον προσωπικό υπολογιστή και καταγράφονται στο /var/log/syslog

```
Dec 5 19:05:52 snf-879210 named[1266]: client [REDACTED] detectportal.firefox.com.georgedebian.com): query: detectportal.firefox.com.georgedebian$
Dec 5 19:05:52 snf-879210 named[1266]: client [REDACTED] detectportal.firefox.com.georgedebian.com): query: detectportal.firefox.com.georgedebian$
Dec 5 19:05:53 snf-879210 named[1266]: client [REDACTED] georgedebian.com): query: georgedebian.com IN A + [REDACTED]
Dec 5 19:05:53 snf-879210 named[1266]: client [REDACTED] georgedebian.com): query: georgedebian.com IN AAAA [REDACTED]
Dec 5 19:05:53 snf-879210 named[1266]: client [REDACTED] example.com): query: example.com IN A + [REDACTED]
Dec 5 19:05:53 snf-879210 named[1266]: client [REDACTED] example.com): query: example.com IN AAAA [REDACTED]
Dec 5 19:06:21 snf-879210 named[1266]: client [REDACTED] push.services.mozilla.com): query: push.services.mozilla.com IN A + [REDACTED]
```

Παρακάτω φαίνεται η λειτουργία του domain example.com

```
root@debian:/home/george# nslookup example.com
Server:
Address: #53

Name: example.com
Address:
Name: example.com
Address: ::1

root@debian:/home/george#
root@debian:/home/george# dig example.com

; <<>> DiG 9.11.5-P4-5.1+deb10u2-Debian <<>> example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37105
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;example.com.                IN      A

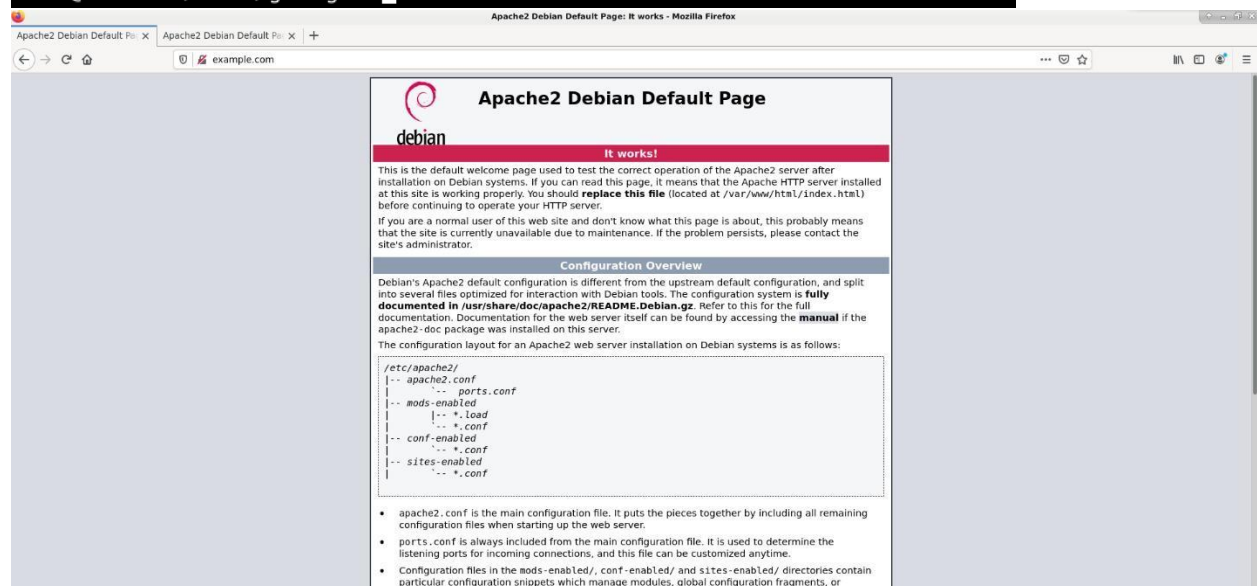
;; ANSWER SECTION:
example.com.                 604800  IN      A      [redacted]

;; AUTHORITY SECTION:
example.com.                 604800  IN      NS      example.com.

;; ADDITIONAL SECTION:
example.com.                 604800  IN      AAAA    ::1

;; Query time: 140 msec
;; SERVER: [redacted]
;; WHEN: Sat Dec 05 20:59:43 EET 2020
;; MSG SIZE rcvd: 98

root@debian:/home/george#
```



Apache2 Debian Default Page: It works! - Mozilla Firefox

Apache2 Debian Default Page: It works! - Mozilla Firefox

example.com

Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented** in `/usr/share/doc/apache2/README.Debian.gz`. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or

Τα αποτελέσματα φαίνονται παρακάτω (δεξιά το python script και αριστερά tcpdump)

```
root@debian:/home/george# sudo tcpdump -v -n host 192.168.1.199
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
16:15:18.014500 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.1.1 tell
192.168.1.199, length 28
16:15:18.018256 ARP, Ethernet (len 6), IPv4 (len 4), Reply 192.168.1.1 is-at e4:fb:5d
:e8:8e:3d, length 46
16:15:18.021069 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto UDP (17), le
ngth 66)
192.168.1.199.5353 > [REDACTED]: 34000- [0q] 0/0/0 (38)
16:16:02.676407 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto UDP (17), le
ngth 66)
192.168.1.199.5353 > [REDACTED]: 34000- [0q] 0/0/0 (38)
16:16:03.587422 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto UDP (17), le
ngth 66)
192.168.1.199.5353 > [REDACTED]: 34000- [0q] 0/0/0 (38)
16:16:03.803771 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto UDP (17), le
ngth 66)
192.168.1.199.5353 > [REDACTED]: 34000- [0q] 0/0/0 (38)
16:16:03.957062 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto UDP (17), le
ngth 66)
192.168.1.199.5353 > [REDACTED]: 34000- [0q] 0/0/0 (38)
16:16:04.886712 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto UDP (17), le
ngth 66)
192.168.1.199.5353 > [REDACTED]: 34000- [0q] 0/0/0 (38)
16:16:05.085779 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto UDP (17), le
ngth 66)
192.168.1.199.5353 > [REDACTED]: 34000- [0q] 0/0/0 (38)
16:16:05.249940 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto UDP (17), le
ngth 66)
192.168.1.199.5353 > [REDACTED]: 34000- [0q] 0/0/0 (38)
16:16:05.938726 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto UDP (17), le
ngth 66)
192.168.1.199.5353 > [REDACTED]: 34000- [0q] 0/0/0 (38)
16:16:06.170899 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto UDP (17), le
ngth 66)
192.168.1.199.5353 > [REDACTED]: 34000- [0q] 0/0/0 (38)
```

```
root@debian:/home/george/Desktop# python dns_fake_response.py
Begin emission:
Finished sending 1 packets.

Received 1404 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.

Received 2 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.

Received 0 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.

Received 0 packets, got 0 answers, remaining 1 packets
```