

# COMUNICAZIONE TRA DUE MACCHINE

Il report di oggi si tratta di far comunicare due macchine virtuali tra un sito web, e catturando la richiesta con WIRESHARK.

Configuro inetsim su Kali:

1. Attivo https e Dns:

```
#
start_service dns
#start_service http
start_service https
#start_service smtp
```

2. Attivo service:

```
#####
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 192.168.50.100
#
service_bind_address 192.168.32.100
```

3. Attivo il dns port:

```
#####
# Service DNS
#####
# dns_bind_port
#
# Port number to bind DNS service to
#
# Syntax: dns_bind_port <port number>
#
# Default: 53
#
dns_bind_port 53
```

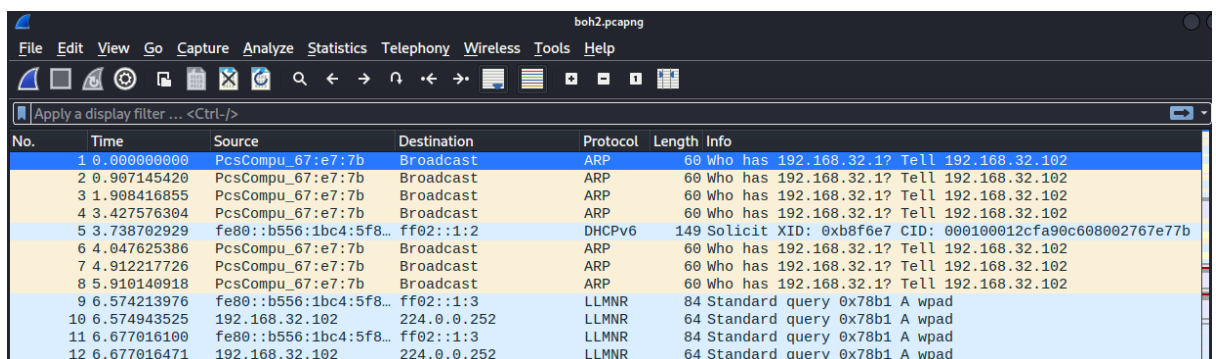
4. Attivo Dns default domainname:

```
#####
# dns_default_domainname
#
# Default domain name to return with DNS replies
#
# Syntax: dns_default_domainname <domain name>
#
# Default: inetsim.org
#
dns_default_domainname epicode.internal
```

5. Attivo il sito web (DNS static):

```
#####  
# dns_static  
#  
# Static mappings for DNS  
#  
# Syntax: dns_static <fqdn hostname> <IP address>  
#  
# Default: none  
#  
dns_static www.epicode.internal 192.168.32.100  
#dns_static ns1.foo.com 10.70.50.30  
#dns_static ftp.bar.net 10.10.20.30
```

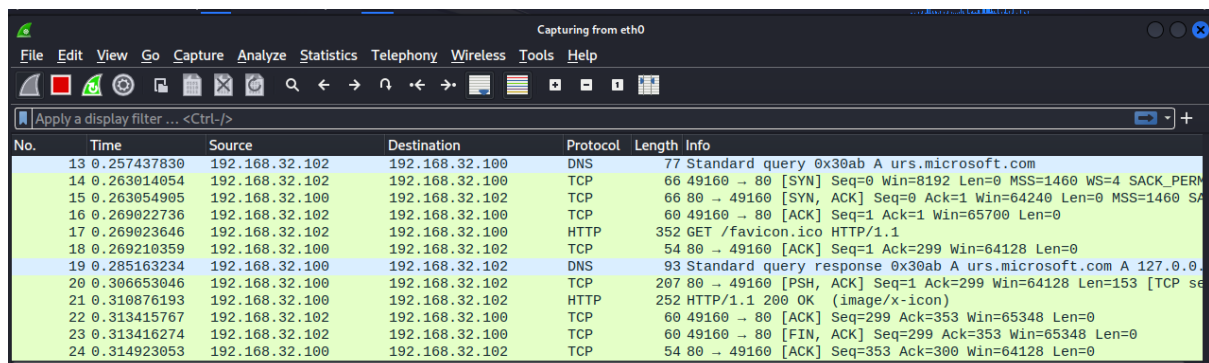
6. Faccio la cattura con wireshark:



The image shows a Wireshark capture of network traffic. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu_67:e7:7b	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.102
2	0.907145420	PcsCompu_67:e7:7b	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.102
3	1.908416855	PcsCompu_67:e7:7b	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.102
4	3.427576394	PcsCompu_67:e7:7b	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.102
5	3.738702929	fe80::b556:1bc4:5f8...	ff02::1:2	DHCPv6	149	Solicit XID: 0xb8f6e7 CID: 000100012cfa90c608002767e77b
6	4.047625386	PcsCompu_67:e7:7b	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.102
7	4.912217726	PcsCompu_67:e7:7b	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.102
8	5.910140918	PcsCompu_67:e7:7b	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.102
9	6.574213976	fe80::b556:1bc4:5f8...	ff02::1:3	LLMNR	84	Standard query 0x78b1 A wpad
10	6.574943525	192.168.32.102	224.0.0.252	LLMNR	64	Standard query 0x78b1 A wpad
11	6.677016100	fe80::b556:1bc4:5f8...	ff02::1:3	LLMNR	84	Standard query 0x78b1 A wpad
12	6.677016471	192.168.32.102	224.0.0.252	LLMNR	64	Standard query 0x78b1 A wpad

Dopo questi passaggi, rimetto il cancelletto davanti a https e tolgo da http, e rifaccio la cattura su wireshark



The image shows a Wireshark capture of network traffic. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
13	0.257437830	192.168.32.102	192.168.32.100	DNS	77	Standard query 0x30ab A urs.microsoft.com
14	0.263014054	192.168.32.102	192.168.32.100	TCP	66	49160 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
15	0.263054905	192.168.32.100	192.168.32.102	TCP	66	80 → 49160 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SA
16	0.269022736	192.168.32.102	192.168.32.100	TCP	60	49160 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
17	0.269023646	192.168.32.102	192.168.32.100	HTTP	352	GET /favicon.ico HTTP/1.1
18	0.269210359	192.168.32.100	192.168.32.102	TCP	54	80 → 49160 [ACK] Seq=1 Ack=299 Win=64128 Len=0
19	0.285163234	192.168.32.100	192.168.32.102	DNS	93	Standard query response 0x30ab A urs.microsoft.com A 127.0.0.1
20	0.306653046	192.168.32.100	192.168.32.102	TCP	207	80 → 49160 [PSH, ACK] Seq=1 Ack=299 Win=64128 Len=153 [TCP se
21	0.310876193	192.168.32.100	192.168.32.102	HTTP	252	HTTP/1.1 200 OK (image/x-icon)
22	0.313415767	192.168.32.102	192.168.32.100	TCP	60	49160 → 80 [ACK] Seq=299 Ack=353 Win=65348 Len=0
23	0.313416274	192.168.32.102	192.168.32.100	TCP	60	49160 → 80 [FIN, ACK] Seq=299 Ack=353 Win=65348 Len=0
24	0.314923053	192.168.32.100	192.168.32.102	TCP	54	80 → 49160 [ACK] Seq=353 Ack=300 Win=64128 Len=0

**NOTE:** Quello che si vede subito in comparazione con http e https, e che quando fai la richiesta per entrare nel sito su windows 7, ci mette molto a caricarsi la pagina web, e prima di entrare, win7 ti chiede se vuoi veramente entrare nella pagina come forma di sicurezza, infatti si vede su wireshark che ti viene fuori una riga rossa, che è quella di permesso, invece su http entra molto veloce e non ti chiede niente. Dopo dentro a wireshark si vede la differenza nel http dove già ti fa vedere la richiesta http e il server risponde

**veloce. Invece su https, win7 manda la richiesta al dns, questi fanno lo scambio delle chiavi per l'accesso.**