



Simulazione rete complessa

29/09/23

Davide Diglio

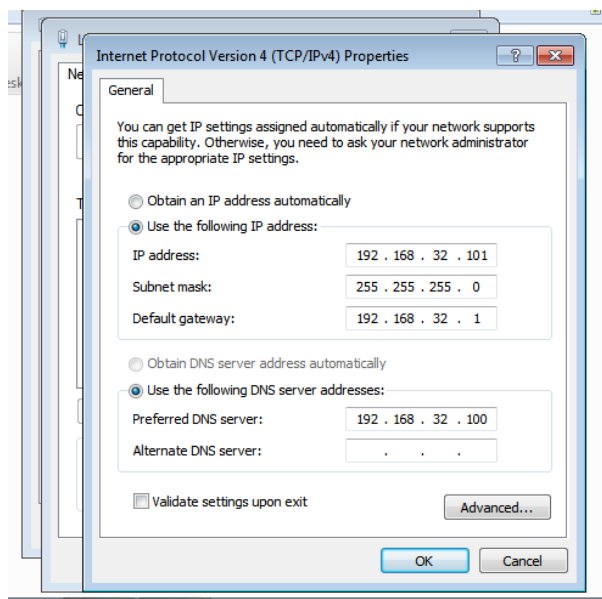
Obiettivi

1. Simulare un'architettura client server in cui l'indirizzo 192.186.32.101 richiede al l'indirizzo 192.168.32.100 un risorsa all'hostname epicode.internal tramite web browser.
2. Intercettare la comunicazione con Wireshark.

Svolgimento

In questo compito l'obiettivo era quello di intercettare la comunicazione tra i due indirizzi, evidenziando i Mac address ed il contenuto del HTTPS o HTTP.

Prima di intercettare la comunicazione si doveva impostare l'IP ai due client server (Kali con 192.168.32.100 e Windows 7 con 192.168.32.101).



Dopodichè su Kali si doveva attivare il servizio DNS impostandolo; ad esempio:

```
#####
# dns_default_ip
#
# Default IP address to return with DNS replies
#
# Syntax: dns_default_ip <IP address>
#
# Default: 127.0.0.1
#
dns_default_ip 192.168.32.100
```

```
#####
service_bind_address
IP address to bind services to
Syntax: service_bind_address <IP address>
Default: 127.0.0.1
service_bind_address 192.168.32.100
```

dopo aver impostato tutto si inizia a intercettare la comunicazione con Wireshark cercando di evidenziare i Mac address e il contenuto della richiesta HTTPS.

The screenshot displays two virtual machines running on Oracle VM VirtualBox. The top window is a Kali Linux VM (kali-linux-2023.3-virtualbox-amd64) showing the Wireshark network protocol analyzer. The bottom window is a Windows 7 VM (Windows 7 [In esecuzione]) showing a default HTML page from the InetSim server.

Wireshark Network Traffic:

No.	Time	Source	Destination	Protocol	Length	Info
48	147.013392769	PcsCompu_00:64:9d	Broadcast	ARP	60	Who has 192.168.32.1? Tel
49	148.013659277	PcsCompu_00:64:9d	Broadcast	ARP	60	Who has 192.168.32.1? Tel
63	151.003208990	PcsCompu_00:64:9d	Broadcast	ARP	60	Who has 192.168.32.1? Tel
65	151.515843879	PcsCompu_00:64:9d	Broadcast	ARP	60	Who has 192.168.32.1? Tel
68	152.516818389	PcsCompu_00:64:9d	Broadcast	ARP	60	Who has 192.168.32.1? Tel
82	257.256803678	PcsCompu_00:64:9d	Broadcast	ARP	60	Who has 192.168.32.100? T
83	257.256814453	PcsCompu_00:64:9d	Broadcast	ARP	60	Who has 192.168.32.100? T
93	257.330632447	PcsCompu_00:64:9d	Broadcast	ARP	60	Who has 192.168.32.1? Tel
95	258.052686696	PcsCompu_00:64:9d	Broadcast	ARP	60	Who has 192.168.32.1? Tel
96	259.053893750	PcsCompu_00:64:9d	Broadcast	ARP	60	Who has 192.168.32.1? Tel
104	263.097080750	PcsCompu_00:64:9d	Broadcast	ARP	60	Who has 192.168.32.1? Tel
105	264.055821194	PcsCompu_00:64:9d	Broadcast	ARP	60	Who has 192.168.32.1? Tel
106	265.056498315	PcsCompu_00:64:9d	Broadcast	ARP	60	Who has 192.168.32.1? Tel
113	772472076	192.168.32.100	192.168.32.255	BROWSER	243	Local Master Announcement
117	384.532680201	fe80::10ae:bd01:bfg...	ff02::1:2	DHCPv6	146	Solicit XID: 0xbda1bd CID
118	384.532708456	fe80::10ae:bd01:bfg...	ff02::1:2	DHCPv6	146	Solicit XID: 0xbda1bd CID
119	386.532857555	fe80::10ae:bd01:bfg...	ff02::1:2	DHCPv6	146	Solicit XID: 0xbda1bd CID
120	318.533252561	fe80::10ae:bd01:bfg...	ff02::1:2	DHCPv6	146	Solicit XID: 0xbda1bd CID
121	318.536645617	fe80::10ae:bd01:bfg...	ff02::1:2	DHCPv6	146	Solicit XID: 0xbda1bd CID
122	334.544229736	fe80::10ae:bd01:bfg...	ff02::1:2	DHCPv6	146	Solicit XID: 0xbda1bd CID
66	152.016815899	192.168.32.101	192.168.32.100	DNS	90	Standard query 0xa21b A w
67	152.041377295	192.168.32.100	192.168.32.101	DNS	106	Standard query response 0
1	0.000000000	192.168.32.101	192.168.32.100	ICMP	74	Echo (ping) request id=0
2	0.000017807	192.168.32.100	192.168.32.101	ICMP	74	Echo (ping) reply id=0
3	0.987668944	192.168.32.101	192.168.32.100	ICMP	74	Echo (ping) request id=0
4	0.987699182	192.168.32.100	192.168.32.101	ICMP	74	Echo (ping) reply id=0
5	1.987873785	192.168.32.101	192.168.32.100	ICMP	74	Echo (ping) request id=0
6	1.987890240	192.168.32.100	192.168.32.101	ICMP	74	Echo (ping) reply id=0
7	2.988998348	192.168.32.101	192.168.32.100	ICMP	74	Echo (ping) request id=0
8	2.989127776	192.168.32.100	192.168.32.101	ICMP	74	Echo (ping) reply id=0
27	143.746168482	fe80::10ae:bd01:bfg...	ff02::1:3	LLMNR	84	Standard query 0x3ca9 A w

Windows 7 VM: The screenshot shows a Windows 7 desktop with Internet Explorer open. The address bar shows the URL <http://192.168.32.100/>. The page content displays the default HTML page for InetSim HTTP server fake mode, stating: "This is the default HTML page for InetSim HTTP server fake mode. This file is an HTML document."

Conclusione

Questa simulazione abbiamo visto come intercettare la comunicazione tramite Wireshark e come impostare un server DNS e attivare anche i server HTTP/HTTPS che sono dei protocolli di comunicazione tra client e un server web e la principale differenza è che HTTPS è più sicuro, perchè in forma criptata.