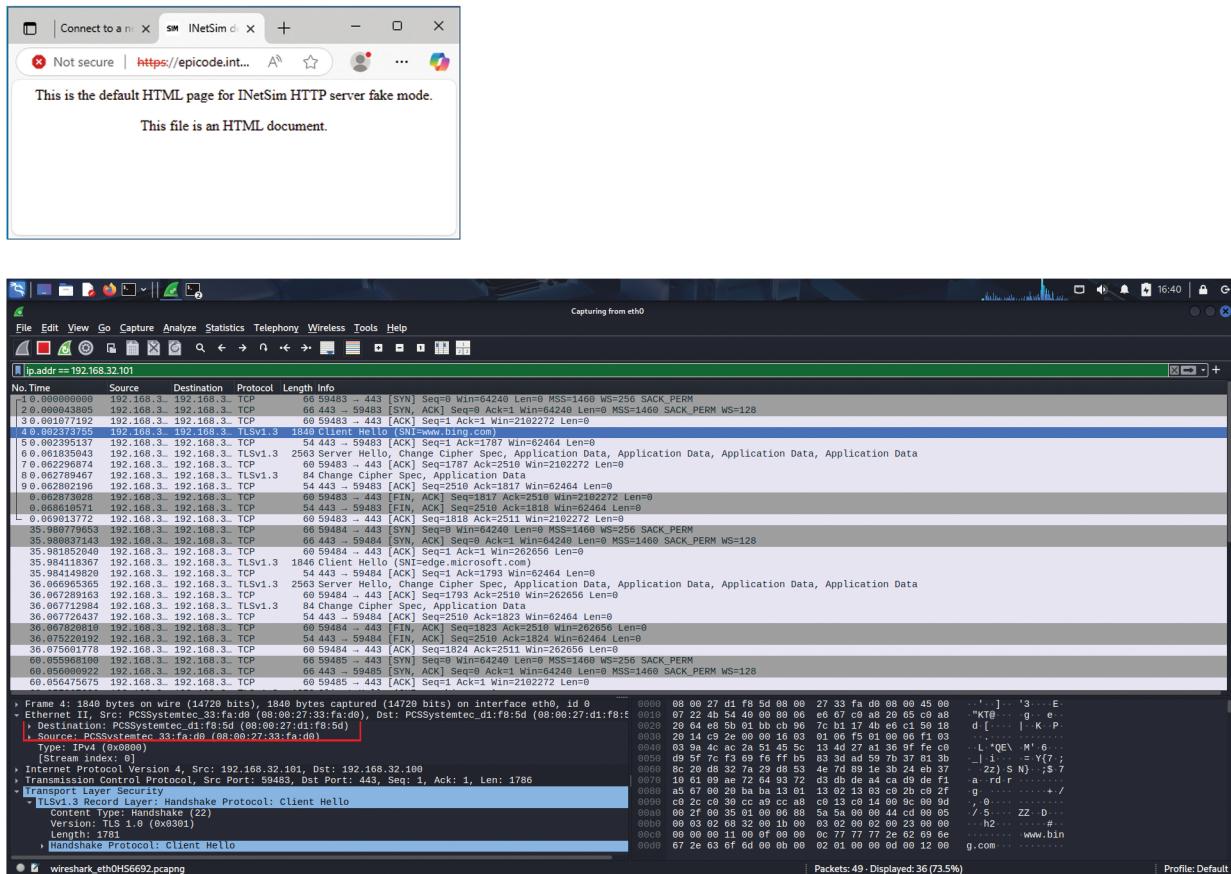


Emy Mangogna - W4D4 - Pratica

Simulazione di un'architettura client-server in ambiente di laboratorio virtuale, con un client Windows (**192.168.32.101**) e un server Kali (**192.168.32.100**) che esegue iNetSim per emulare servizi di rete (DNS, HTTP, HTTPS).

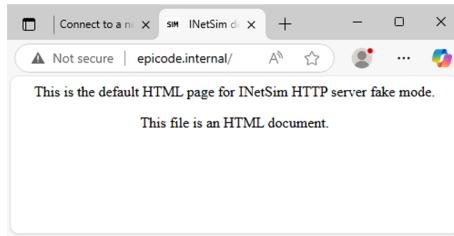
```
(kali㉿kali)-[~]
$ sudo inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory:      /var/log/inetsim/
Using data directory:     /var/lib/inetsim/
Using report directory:   /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Warning: Unknown option 'Service' in configuration file '/etc/inetsim/inetsim.conf' line 368
Configuration file parsed successfully.
== INetSim main process started (PID 53465) ==
Session ID: 53465
Listening on: 0.0.0.0
Real Date/Time: 2025-07-24 15:42:49
Fake Date/Time: 2025-07-24 15:42:49 (Delta: 0 seconds)
Forking services...
* dns_53_tcp_udp - started (PID 53477)
* http_80_tcp - started (PID 53478)
* https_443_tcp - started (PID 53479)
done.
Simulation running.
```

Cattura del traffico generato da una richiesta HTTPS del client Windows verso episode.internal utilizzando Wireshark.



I MAC address di sorgente e destinazione risultano visibili nella sezione Ethernet II, mentre il contenuto della richiesta è cifrato, come evidenziato dalla presenza di pacchetti TLS (Encrypted Application Data)

Cattura del traffico generato da una richiesta HTTP del client Windows verso episode.internal. I MAC address sono visibili nella sezione Ethernet II e, a differenza del traffico HTTPS, il contenuto della richiesta (metodo GET, intestazioni Host e User-Agent) risulta leggibile in chiaro, mostrando la mancanza di cifratura.



No. Time	Source	Destination	Protocol	Length	Info
4. 4.285747278	192.168.3. 192.168.3..	192.168.3..	HTTP	312	HTTP/1.1 200 OK (text/html)
4. 4.256423677	192.168.3..	192.168.3..	HTTP	622	GET /captivewortal/generate_204 HTTP/1.1
4. 288247159	192.168.3..	192.168.3..	HTTP	312	HTTP/1.1 200 OK (text/html)
5. 404422959	192.168.3..	192.168.3..	HTTP	312	HTTP/1.1 200 OK (text/html)
5. 404422959	192.168.3..	192.168.3..	HTTP	312	HTTP/1.1 200 OK (text/html)
5. 415895329	192.168.3..	192.168.3..	HTTP	250	GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?b0cdic63270e238d HTTP/1.1
5. 448571655	192.168.3..	192.168.3..	HTTP	312	HTTP/1.1 200 OK (text/html)
5. 543149327	192.168.3..	192.168.3..	HTTP	250	GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?c74c63be3b81b4 HTTP/1.1
5. 543149327	192.168.3..	192.168.3..	HTTP	312	HTTP/1.1 200 OK (text/html)
5. 676743998	192.168.3..	192.168.3..	HTTP	250	GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?15b0b351251bce22 HTTP/1.1
5. 7064772446	192.168.3..	192.168.3..	HTTP	312	HTTP/1.1 200 OK (text/html)
5. 799333385	192.168.3..	192.168.3..	HTTP	250	GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?d12919f0f2e564e HTTP/1.1
5. 8310772571	192.168.3..	192.168.3..	HTTP	312	HTTP/1.1 200 OK (text/html)
5. 86007872571	192.168.3..	192.168.3..	HTTP	250	GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?74cf75b469fc4996 HTTP/1.1
5. 86026518339	192.168.3..	192.168.3..	HTTP	312	HTTP/1.1 200 OK (text/html)
5. 86109765516	192.168.3..	192.168.3..	HTTP	250	GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?89dd7185f92722a HTTP/1.1
5. 86127366961	192.168.3..	192.168.3..	HTTP	312	HTTP/1.1 200 OK (text/html)
Frame 71: 511 bytes on wire (4088 bits), 511 bytes captured (4088 bits) on interface eth0, id 0				0x0030	20 14 9c f7 00 00 47 45 54 28 2f 20 48 54 54 58
Ethernet II Src: PCSSystemtec_33:fa:d0 (08:00:27:33:fa:d0), Dst: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d)				0x0040	2f 31 2e 31 0d 08 4f 6f 73 74 3a 20 65 70 69 63
Destination: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d)				0x0050	73 74 3a 20 65 70 69 63 00 00 00 00 00 00 00 00
Type: IPv4 (0x0800)				0x0060	64 65 63 74 66 6f 6e 6a 20 65 65 70 2d 61
[Stream index: 0]				0x0070	6c 69 76 05 0d 06 55 78 67 72 61 64 65 2d 49 66
Internet Protocol Version 4, Src: 192.168.32.181, Dst: 192.168.32.100				0x0080	73 65 63 75 72 65 25 52 65 71 75 65 73 74 3a
Transmission Control Protocol, Src Port: 59448, Dst Port: 80, Seq: 1, Ack: 1, Len: 457				0x0090	73 74 3a 20 65 65 70 69 63 00 00 00 00 00 00 00
HTTP/1.1 [TCP segment of a connection]				0x00a0	64 6f 77 73 20 4e 54 20 31 39 2e 39 30 20 57 69
GET / HTTP/1.1\r\n				0x00b0	6e 30 34 3b 20 78 34 34 29 28 41 76 79 60 65 57
Host: episode.internal\r\n				0x00c0	65 62 4b 69 74 2f 35 33 37 2e 33 36 29 2d 4b 48
Connection: keep-alive\r\n				0x00d0	69 65 63 74 66 6f 6e 6a 20 65 65 70 2d 61
Upgrade-Insecure-Requests: 1\r\n\r\n				0x00e0	60 68 67 6d 65 2f 31 33 38 2e 39 2e 30 60 6a 41
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.6757.136 Safari/537.36				0x00f0	20 68 67 6d 65 2f 31 33 38 2e 39 2e 30 60 6a 41
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8				0x0100	30 20 53 01 66 61 72 09 2f 35 33 37 2e 33 36 20
Accept-Encoding: gzip, deflate\r\n				0x0110	45 64 67 2f 31 33 38 2e 30 2e 38 2e 30 60 6a 41
Accept-Language: en-US,en;q=0.9,en-GB;q=0.8\r\n				0x0120	03 63 69 74 78 70 74 65 66 74 6d 66 74 6d 66
\r\n				0x0130	60 6c 2b 78 6d 6c 2c 61 70 78 66 69 63 61 74 69
[Response in Frame: 78]				0x0140	66 6c 2b 78 6d 6c 2c 61 70 78 66 69 63 61 74 69
Full request URI: http://episode.internal/				0x0150	6f 6e 2f 78 6d 6c 3b 71 3d 38 2e 39 2e 60 6d 61
				0x0160	67 65 2f 61 76 69 66 2c 69 6d 61 67 69 2f 77 65
				0x0170	02 67 65 3b 76 3d 62 33 3b 71 3d 38 2e 37 60 6a
				0x0180	6f 6e 2f 78 6d 6c 3b 71 3d 38 2e 39 2e 60 6d 61
				0x0190	69 6f 6e 2f 73 69 67 0e 65 64 2d 65 78 63 68 61
				0x01a0	6e 67 65 3b 76 3d 62 33 3b 71 3d 38 2e 37 60 6a