

UNITÀ 2/ COMPITO 1/ SETTIMANA 2

Ho aperto il terminale del pc nativo ed eseguito il comando << arp -a >> per vedere l'ip del modem e l'ip del computer.

Sono andato su kali e ho aperto ettercap così da fare una scansione degli Host una volta fatta chiediamo la lista di quest'ultimi e selezioniamo i target in questo caso il primo è il modem (192.168.1.1) e il secondo il nostro pc (192.168.1.47) e poi avviamo l'ARP-Poisoning e per simulare e verificare che funzioni usiamo vulnweb.



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

[Browse categories](#)

[Browse artists](#)

[Your cart](#)

[Signup](#)

[Your profile](#)

[Our guestbook](#)

[AJAX Demo](#)

Links

[Security art](#)

[PHP scanner](#)

[PHP vuln help](#)

[Fractal Explorer](#)



If you are already registered please enter your login information below:

Username :

Password :

You can also [signup here](#).

Signup disabled. Please use the username **test** and the password **test**.

[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

```
kali-linux-2023.3-virtualbox-amd64 [in esecuzione] - Oracle VM VirtualBox
File Macchine Visualizza Inserimento Dispositivi Auto
1 2 3 4 e
Ettercap
0.8.3.1 (EB)

Host List x
IP Address MAC Address Description
192.168.1.1 10:13:01:EF:B3:26
192.168.1.3 90:05:6B:1C:D0:41
192.168.1.21 EE:2E:98:44:5F:C2
192.168.1.31 93:1B:17:1F:F5:FC
192.168.1.32 08:00:27:9A:22:5E
192.168.1.47 30:F6:EF:32:DF:25
192.168.1.70 AA:20:3F:F5:CL:76
192.168.1.254 12:13:31:EF:B3:26

Delete Host Add to Target 1 Add to Target 2

Listening on:
eth0 -> 08:00:27:B6:37:C3
192.168.1.14/255.255.255.0
fe80::a0:27ff:feb6:37:c3/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to EUID 65534 EUID 65534...

34 plugins
42 protocol dissectors
57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole network for 255 hosts...
8 hosts added to the hosts list...
Host 192.168.1.1 added to TARGET1
Host 192.168.1.47 added to TARGET2

ARP poisoning victims:

GROUP 1: 192.168.1.1 10:13:31:EF:B3:26
GROUP 2: 192.168.1.47 30:F6:EF:32:DF:25
HTTP - 44.228.249.3:80 -> USER: samuel PASS: ciaociao INFO: http://testphp.vulnweb.com/login.php
```

Così facendo possiamo vedere username e password e tutte queste fasi possiamo riassumerle in quattro:

**1-Ricerca degli host 2-chi è il target
host(modem) e il secondo(computer)**

3-lista degli host

4-arpoisoning

PROTOCOLLO ARP

L'ARP (Address Resolution Protocol) è un protocollo o una procedura che collega un indirizzo IP (Internet Protocol) in continua evoluzione a un indirizzo fisso del computer fisico, noto anche come indirizzo MAC (Media Access Control), in una rete locale (LAN)

ATTACCO ARP-POISONING

Un attacco ARP-poisoning consente di intercettare le comunicazioni tra i dispositivi di rete corrompendo la tabella ARP della rete

ATTACCHI MITM

Sono attacchi informatici per indicare che qualcuno sta segretamente sta ritrasmettendo o comunque alterando la comunicazioni tra due persone che credono di star parlando direttamente tra loro