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.

acunetix acuart

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art

go

- Browse categories
- Browse artists
- Your cart
- Signup
- Your profile
- Our guestbook
- AJAX Demo

Links

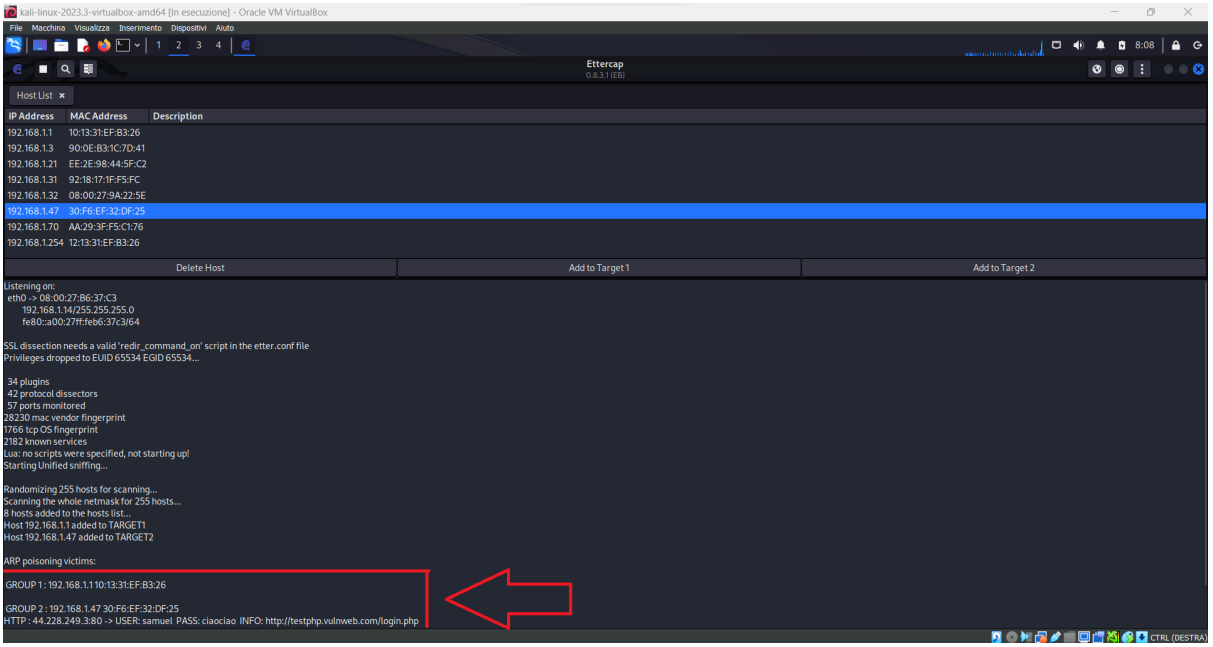
- Security art
- PHP scanner
- PHP vuln help
- Fractal Explorer

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

Username :	samuel
Password :	••••••••
	login

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



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-arpoisong

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