

- **Cos'è il protocollo ARP?**

Il protocollo ARP (Address Resolution Protocol) è un componente essenziale nella comunicazione di rete che consente di mappare gli indirizzi IP (Internet Protocol) degli host su una rete locale agli indirizzi MAC (Media Access Control) corrispondenti. Dunque, il protocollo ARP permette di identificare l'indirizzo fisico (MAC) di un dispositivo quando si conosce il suo indirizzo IP. Per fare ciò, utilizza una tabella chiamata ARP Table.

- **Cosa sono gli attacchi MITM?**

Gli attacchi Man-in-the-Middle (MITM) sono strategie malevoli in cui un attaccante si posiziona tra due parti che comunicano, intercettando o manipolando il flusso di informazioni. L'obiettivo principale di un attacco MITM è ottenere accesso non autorizzato alle informazioni scambiate tra le due parti. Questi attacchi possono verificarsi in varie forme, come la cattura di pacchetti di dati o la modifica delle comunicazioni tra le vittime.

- **Cos'è l'attacco ARP-Poisoning?**

L'ARP-Poisoning, è un tipo di attacco MITM che sfrutta le vulnerabilità nel protocollo ARP. In questo attacco, l'attaccante invia pacchetti ARP falsificati alla rete, modificando la tabella ARP di un dispositivo o di un router. Di conseguenza, il traffico di rete destinato a un particolare indirizzo IP viene dirottato verso l'attaccante.

- **Fasi dell'Attacco ARP-Poisoning con Ettercap:**

- . **Configurazione delle Interfacce di Rete:**

Avviamo Ettercap e configuriamo le interfacce di rete. Specifichiamo l'interfaccia della nostra scheda di rete locale (es. eth0) come interfaccia di ascolto.

- . **Scansione della Rete:**

Eseguiamo una scansione della rete locale con Ettercap per identificare i dispositivi con i rispettivi indirizzi IP.

- . **Selezione delle Vittime:**

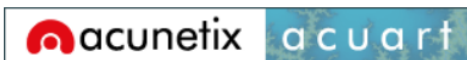
Selezioniamo la vittima che vogliamo indirizzare con l'attacco ARP-Poisoning utilizzando l'interfaccia di Ettercap (Target 1 indirizzo ip router gateway che fungerà da server, Target 2 indirizzo ip della vittima).

- . **Avvio dell'Attacco ARP-Poisoning:**

Una volta selezionate le vittime, avviamo l'attacco ARP-Poisoning. Ettercap invierà pacchetti ARP falsificati alla rete, associando il proprio indirizzo MAC all'indirizzo IP della vittima.

- . **Cattura del Traffico:**

Ettercap ora funge da intermediario tra la vittima e il router. Tutto il traffico tra di essi passerà attraverso l'attaccante. Questo consente all'attaccante di catturare e analizzare il traffico di rete, nel nostro caso siamo riusciti a carpire le credenziali di accesso alla pagina di login di 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

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**.

IP Address	MAC Address	Description
fe80::7eff:4dff:fe72:33bd	7C:FF:4D:72:33:BD	
192.168.1.1	7C:FF:4D:72:33:BD	
192.168.1.49	00:1D:60:CB:07:13	
192.168.1.53	0C:9A:3C:4B:9C:F4	
Delete Host		
Host 192.168.1.1 added to TARGET1		
Host 192.168.1.53 added to TARGET2		
ARP poisoning victims:		
GROUP 1 : 192.168.1.1 7C:FF:4D:72:33:BD		
GROUP 2 : 192.168.1.53 0C:9A:3C:4B:9C:F4		
HTTP : 44.228.249.3:80 -> USER: ciao PASS: ciaoo INFO: http://testphp.vulnweb.com/lo		
CONTENT: uname=ciao&pass=ciaoo		

TABELLA ARP PRIMA ARP POISONING:

Interfaccia: 192.168.1.53 --- 0x12		
Indirizzo Internet	Indirizzo fisico	Tipo
192.168.1.1	7c-ff-4d-72-33-bd	dinamico
192.168.1.56	08-00-27-cb-7e-f5	dinamico

TABELLA ARP DOPO ARP POISONING:

Indirizzo Internet	Indirizzo fisico	Tipo
192.168.1.1	08-00-27-cb-7e-f5	dinamico
192.168.1.56	08-00-27-cb-7e-f5	dinamico

Dopo aver fatto l'ARP poisoning, il dispositivo vittima associa all'indirizzo ip del router gateway l'indirizzo MAC della macchina attaccante.