S6/L1

Traccia: Utilizzando Ettercap andiamo a simulare un attacco ARP-Poisoning. La macchina web vittima è a piacere, in alternativa si può usare: vulnweb. http://testphp.vulnweb.com/login.php Fare un report su:

1- Cos’è il protocollo ARP.

2- Cosa sono gli attacchi MITM.

3- Cos’è l'attacco ARP-Poisoning.

4- Le fasi dell'attacco.

1. Protocollo ARP (address resolution protocol)

È un protocollo di rete utilizzato per associare un indirizzo IP a un indirizzo fisico (MAC address). Quando un dispositivo sulla rete vuole inviare dati a un altro dispositivo, deve conoscere l'indirizzo MAC del destinatario. L'ARP viene utilizzato per scoprire questo indirizzo. Il processo inizia quando un dispositivo invia una richiesta ARP broadcast chiedendo chi ha quel determinato IP.

Tutti i dispositivi sulla stessa rete ricevono la richiesta, ma solo il dispositivo con l'indirizzo IP corrispondente risponderà con il proprio indirizzo MAC. Verrà salvata la coppia IP – MAC nella propria ARP cache, ovvero una tabella con le coppie IP – MAC salvate per futuri utilizzi.

1. Attacchi MITM

Un attacco Man-in-the-Middle è un tipo di attacco informatico in cui un attaccante si posiziona tra due parti che stanno comunicando, cercando di intercettare e manipolare in modo attivo la comunicazione tra di loro. Gli obiettivi di un attacco MITM sono quelli di intercettare e ottenere informazioni sensibili e quindi di compromettere l'integrità della comunicazione; di far crashare la connessione, di attivare una sostituzione, ovvero “far credere al client di raggiungere il vero server e viceversa” fino ad arrivare ad una possibile infiltrazione di malware nei dispositivi della comunicazione. Questo tipo di attacco è pericoloso perché spesso avviene senza che le parti ne siano consapevoli.

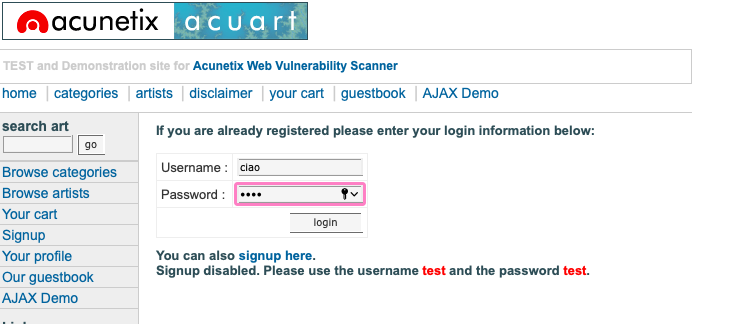
Due tipi di attacco MITM sono: l’ARP poisoning e DNS poisoning.

1. Attacco ARP-poisoning

L'ARP poisoning è una tecnica di attacco in cui un attaccante invia pacchetti ARP falsificati all'interno di una rete locale. L'obiettivo è di corrompere o manipolare la tabella ARP di un dispositivo di destinazione, facendo associare un indirizzo IP a un indirizzo MAC controllato dall'attaccante.

Per difendersi contro l'ARP poisoning, è possibile adottare misure di sicurezza come l'uso di connessioni crittografate (HTTPS).

1. Le fasi dell’attacco
2. Per prima cosa, apriamo un tool già impostato su kali, ovvero ETTERCAP, è uno strumento utile per l’esecuzione di un attacco MITM per intercettare le comunicazioni e per indirizzare il traffico verso l’attaccante.
3. Su Ettercap aggiungiamo i nostri due target: il primo IP target è l’IP del router (in questo caso) o del server, mentre per il secondo IP target utilizziamo nel caso specifico quello del nostro PC. Importante ricordare che devono trovarsi sulla stessa rete, infatti è un tipo di attacco che avviene in modalità white box, ovvero bisogna essere all’interno dell’edificio dove avviene l’attacco e collegato alla rete. Una volta inseriti i target, avviamo la scansione dell’ARP poisoning.
4. Come prossimo step, per vedere se ha funzionato, andiamo su un sito non criptato (in questo caso usiamo vulnweb) e inseriamo le credenziali per un login:



1. Torniamo su Ettercap e come dimostra l’immagine sottostante, ha intercettato le credenziali da noi inserite, in chiaro: unname&pass.