ESERCIZIO S6/L1

Utilizzando Ettercap andiamo a simulare un attacco ARP-Poisoning. La macchina web vittima è a piacere, in alternativa si può usare: vulnweb.
Fare un report su: ● Cos'è il protocollo ARP. ● Cosa sono gli attacchi MITM. ● Cos'è l'attacco ARP-Poisoning. ● Le fasi dell'attacco.

Il **protocollo ARP**, acronimo di Address Resolution Protocol, è un protocollo di rete utilizzato per associare un indirizzo di livello di collegamento (come un indirizzo MAC) a un indirizzo IP. Il suo scopo principale è quello di fornire un meccanismo per la traduzione degli indirizzi di rete, consentendo ai dispositivi di comunicare efficacemente all'interno di una rete locale.
Ecco come funziona il protocollo ARP:
- **Richiesta ARP** (ARP Request):
Quando un dispositivo all'interno di una rete deve inviare dati a un altro dispositivo, ma conosce solo l'indirizzo IP di destinazione, invia una richiesta ARP in broadcast.
La richiesta ARP contiene l'indirizzo IP del dispositivo di destinazione e chiede quale sia il suo indirizzo MAC.
- **Risposta ARP** (ARP Reply):
Il dispositivo di destinazione, se è attivo sulla rete, risponde con un messaggio ARP in cui fornisce il proprio indirizzo MAC associato all'indirizzo IP richiesto.
La risposta ARP è inviata solo al dispositivo che ha inizialmente emesso la richiesta ARP.
- **Aggiornamento delle tabelle ARP**:
I dispositivi che ricevono una risposta ARP aggiornano le proprie tabelle ARP. Queste tabelle contengono le associazioni tra indirizzi IP e indirizzi MAC dei dispositivi presenti sulla stessa rete locale.
Le tabelle ARP vengono utilizzate per evitare di dover eseguire nuovamente la procedura ARP per la stessa coppia IP/MAC ogni volta che è necessario comunicare con un dispositivo specifico.
- **Caching ARP**:
Poiché le associazioni IP/MAC possono rimanere costanti per un certo periodo di tempo, le tabelle ARP sono spesso memorizzate nella cache per evitare la necessità di eseguire richieste ARP ogni volta che si deve comunicare con un dispositivo noto.
In sintesi, il protocollo ARP è fondamentale per garantire che i dispositivi in una rete locale possano comunicare tra loro efficacemente, poiché consente la traduzione degli indirizzi IP, che sono utilizzati per l'instradamento dei pacchetti, negli indirizzi MAC, necessari per la comunicazione diretta a livello di collegamento.

Un attacco **Man-in-the-Middle** (MITM) è una forma di attacco informatico in cui un attaccante si posiziona tra due parti che stanno cercando di comunicare tra loro. L'obiettivo principale dell'attaccante è intercettare, modificare o manipolare il flusso di informazioni tra le due parti senza che esse lo sappiano. Gli attacchi MITM possono verificarsi su diversi livelli della pila di protocolli di comunicazione, e possono coinvolgere varie tecniche e vettori d'attacco. Ecco alcuni esempi di attacchi MITM:
- **Intercettazione del Traffico**:
L'attaccante si posiziona fisicamente o logicamente tra il mittente e il destinatario e intercetta il traffico di dati che passa attraverso di lui. Questo può includere l'intercettazione di comunicazioni su reti non protette o l'utilizzo di strumenti come sniffer di rete per catturare dati sensibili.

- **Attacchi ARP Spoofing**:
L'attaccante invia falsi pacchetti ARP (Address Resolution Protocol) alla rete locale per associare il proprio indirizzo MAC a un indirizzo IP legittimo. In questo modo, l'attaccante può intercettare il traffico destinato a un altro dispositivo nella rete.
- **Phishing**:
L'attaccante crea siti web o invia messaggi di posta elettronica contraffatti per indurre la vittima a rivelare informazioni sensibili come nome utente, password o dati finanziari. In questo caso, l'attaccante si trova "in mezzo" tra l'utente e il sito web legittimo.
- **Session Hijacking**:
L'attaccante ruba l'identificatore di sessione di un utente autenticato per assumere il controllo di una sessione di comunicazione già stabilita. Ciò può consentire all'attaccante di accedere a informazioni riservate o compiere azioni a nome dell'utente legittimo.
- **DNS Spoofing**:
L'attaccante manipola le risposte DNS per indirizzare la vittima a un sito web falso anziché al sito legittimo desiderato. Questo può essere usato per condurre attacchi di phishing o per intercettare le comunicazioni.
- **SSL Stripping**:
L'attaccante rimuove la crittografia SSL/TLS da una connessione sicura tra il client e il server, esponendo così i dati sensibili alla visualizzazione e manipolazione.
- **Proxy/MITM sui Livelli Applicativi**:
L'attaccante utilizza un proxy per intercettare e manipolare le comunicazioni tra un'applicazione e un server.
- **Attacchi su reti wireless**:
Gli attacchi MITM possono verificarsi facilmente su reti Wi-Fi non sicure, dove l'attaccante può posizionarsi tra il dispositivo e il punto di accesso per intercettare o manipolare il traffico.
Per proteggersi dagli attacchi MITM, è fondamentale utilizzare tecniche di crittografia, autenticazione robusta e adottare misure di sicurezza, come reti virtuali private (VPN) e certificati SSL/TLS. Inoltre, l'istruzione degli utenti su pratiche di sicurezza informatica è essenziale per prevenire il successo di attacchi come il phishing.

L'**ARP poisoning**, noto anche come ARP spoofing, è una forma di attacco Man-in-the-Middle (MITM) che sfrutta debolezze nel protocollo ARP (Address Resolution Protocol) per compromettere la comunicazione di rete. Questo attacco coinvolge la manipolazione delle tabelle ARP, che associano gli indirizzi IP agli indirizzi MAC nei dispositivi di rete. Ecco una spiegazione più dettagliata di come funziona l'attacco ARP poisoning.
- **Come funziona ARP poisoning**:
Nell'ARP poisoning, un attaccante invia falsi pacchetti ARP sulla rete locale, comunicando agli altri dispositivi che l'indirizzo MAC associato a un determinato indirizzo IP è quello dell'attaccante anziché il legittimo.
- **Fasi dell'attacco**:
- **ARP Request**:
Un dispositivo nella rete invia una richiesta ARP broadcast chiedendo l'indirizzo MAC associato a un determinato indirizzo IP.
- **ARP Reply** (Poisoned):
L'attaccante risponde con un pacchetto ARP contenente un indirizzo MAC falso, affermando di essere il dispositivo associato all'indirizzo IP richiesto.
- **Tabella ARP Corrotta**:

La tabella ARP del dispositivo richiedente viene aggiornata con l'indirizzo MAC fornito dall'attaccante anziché con quello legittimo.
- **Implicazioni dell'attacco**:
Una volta che la tabella ARP di una macchina è stata corrotta, questa comincerà a instradare il traffico destinato all'indirizzo IP legittimo attraverso l'indirizzo MAC falsificato fornito dall'attaccante.
L'attaccante può quindi intercettare, modificare o inoltrare il traffico tra le macchine coinvolte a sua discrezione.
- **Scenari di utilizzo**:
ARP poisoning può essere utilizzato per condurre attacchi MITM su reti locali, consentendo all'attaccante di intercettare o manipolare il traffico tra dispositivi.
Può essere utilizzato per eseguire attacchi di sniffing su reti non crittografate, consentendo all'attaccante di raccogliere informazioni sensibili come username e password.
- **Difese contro ARP poisoning**:
L'utilizzo di protocolli di sicurezza come HTTPS o VPN può aiutare a proteggere il traffico da essere intercettato. L'implementazione di tecniche di rilevamento di ARP poisoning può contribuire a identificare e mitigare gli attacchi. Monitoraggio costante delle tabelle ARP e dell'attività di rete è necessario per individuare anomalie.

Le fasi dell'attacco ARP poisoning coinvolgono l'invio di pacchetti ARP falsi per corrompere le tabelle ARP nei dispositivi di una rete locale. Ecco le fasi principali dell'attacco ARP poisoning:
- **Individuazione della Vittima**:
L'attaccante seleziona una vittima all'interno della rete locale. Questa vittima può essere un singolo dispositivo o l'intera rete, a seconda degli obiettivi dell'attaccante.
- **Monitoraggio del Traffico di Rete**:
L'attaccante monitora il traffico di rete per identificare i dispositivi che comunicano tra loro, in particolare quelli per i quali intende effettuare l'ARP poisoning.
- **Generazione di Pacchetti ARP Falsi**:
L'attaccante genera pacchetti ARP falsi contenenti informazioni contraffatte. Questi pacchetti includono un indirizzo IP legittimo e un indirizzo MAC manipolato, indicando che l'indirizzo IP specificato corrisponde all'indirizzo MAC dell'attaccante.
- **Inondazione della Rete con Pacchetti ARP Falsi**:
L'attaccante inonda la rete con pacchetti ARP falsi, inviandoli in broadcast o a specifici dispositivi. Questo è fatto per sovraccaricare le tabelle ARP dei dispositivi nella rete, causando la memorizzazione delle informazioni contraffatte.
- **Aggiornamento delle Tabelle ARP**:
I dispositivi nella rete ricevono i pacchetti ARP falsi e aggiornano le proprie tabelle ARP con le informazioni fornite dall'attaccante. Questo significa che associano l'indirizzo IP della vittima all'indirizzo MAC dell'attaccante.
- **Inizio dell'Interferenza nel Traffico**:
Una volta che le tabelle ARP delle vittime sono corrotte, l'attaccante può iniziare a intercettare, modificare o inoltrare il traffico tra le vittime. Ad esempio, può intercettare informazioni sensibili o condurre attacchi di tipo Man-in-the-Middle.
- **Persistenza e Mantenimento dell'Attacco**:
L'attaccante può continuare a inviare periodicamente pacchetti ARP falsi per mantenere la persistenza dell'attacco nel tempo. Questo è particolarmente rilevante se le tabelle ARP delle vittime vengono ripristinate o aggiornate.

- **Rimozione dell'Attacco**:
Per rimuovere l'attacco ARP poisoning, è necessario fermare l'invio dei pacchetti ARP falsi e aspettare che le tabelle ARP delle vittime vengano ripristinate correttamente. In alcuni casi, potrebbe essere necessario riavviare i dispositivi coinvolti nella rete.
È importante notare che le fasi possono variare a seconda delle specifiche tecniche utilizzate dall'attaccante e delle condizioni della rete. La difesa contro l'ARP poisoning comporta l'implementazione di misure di sicurezza, come l'uso di protocolli crittografati e la rilevazione attiva di attacchi ARP.