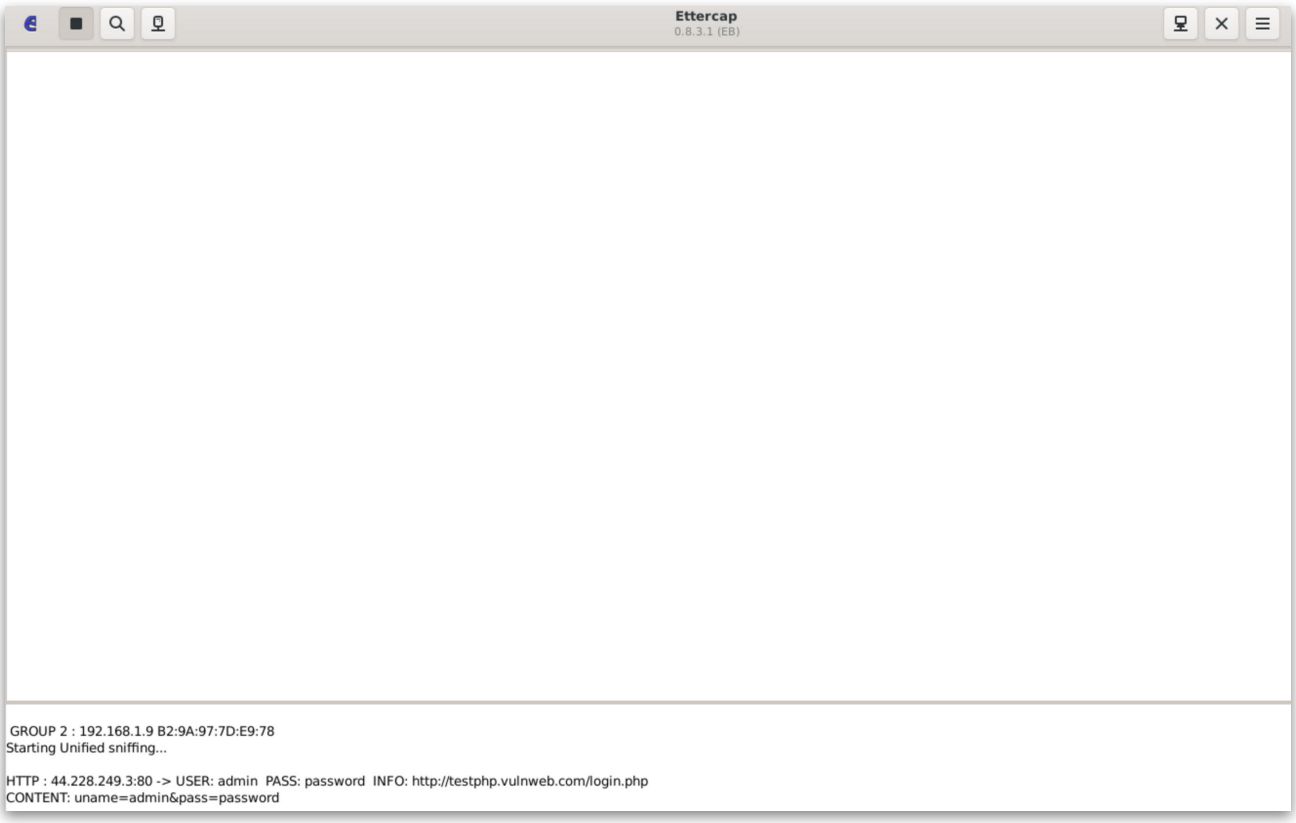
Esercizio W15D1 - Null Session e ARP Poisoning

RICHIESTA

L'esercizio W15D1 si divide in due parti: nella prima, lo studente deve rispondere ad alcuni quesiti relativi alle Null Session e all'ARP Poisoning. Nella seconda parte bisogna invece configurare e utilizzare il tool **Ettercap** per portare a compimento un attacco "Man-in-the-Middle"

~~~

SOLUZIONE

Le **NULL Session** sono connessioni anonime non autenticate stabilite tra un client e un server Windows, tramite il protocollo SMB. In origine, il loro scopo era quello di consentire l'accesso a risorse pubbliche - ad esempio stampanti o file server - senza credenziali. La loro pericolosità è dovuta al fatto che permettono a un attaccante di enumerare informazioni sul sistema target, come nomi utente, condivisioni di rete, patch installate, gruppi e altre risorse.

Ad essere maggiormente esposti alle problematiche legate alle NULL Session sono i sistemi operativi Windows più vecchi, come **Windows XP** o Windows Server 2003. Da Windows Vista in poi, le impostazioni predefinite dei sistemi operativi sono diventate molto più severe in tema di NULL Session, mitigando di molto il problema. Una configurazione sbagliata dei sistemi può però rendere vulnerabili alle NULL Session anche **sistemi operativi Windows più moderni** di XP, come ad esempio 7.

Oltre all'utilizzo di sistemi operativi moderni, la mitigazione principale per questa vulnerabilità è il disabilitare o limitare drasticamente la possibilità di stabilire NULL Session e l'enumerazione di informazioni tramite esse, configurando opportunamente le policy di sicurezza del sistema operativo.

L'**ARP Poisoning** è una tecnica di attacco che sfrutta una vulnerabilità del protocollo ARP, protocollo responsabile della corrispondenza di indirizzo IP e indirizzo MAC delle macchine sulla rete. L'ARP è una funzione fondamentale per fare in modo che le macchine possano parlare fra loro. L'**ARP Poisoning** consiste nell'invio di messaggi ARP falsificati nella rete, così da indurre la macchina target a credere che il MAC address dell'attaccante sia il MAC address legittimo del Gateway e il Gateway stesso a credere che l'indirizzo dell'attaccante sia quello legittimo della macchina target.

In questo modo, tutto il traffico che le due parti si scambiano viene reindirizzato attraverso la macchina dell'attaccante. Quest'ultimo potrà così intercettare facilmente e potenzialmente modificare il traffico. Siamo di fronte, in questo caso, a un attacco **Man-in-the-Middle**.

Essendo il protocollo ARP uno di quelli indispensabili per il funzionamento delle reti, tutti i sistemi operativi sono potenzialmente esposti alla tecnica di ARP Poisoning. La soluzione più immediata per mitigare eventuali attacchi Man-in-the-Middle consiste nel **cifrare il traffico**, utilizzando protocolli come HTTPS che, appunto, cifrano i dati. Anche la **segmentazione della rete** può mitigare l'ARP Poisoning.

Per la seconda parte dell'esercizio, ho innanzitutto installato sulla VM Debian il tool **Ettercap**. Questo programma consente di portare facilmente a termine degli attacchi Man-in-the-Middle (MITM), cioè degli attacchi in cui l'attaccante - nel nostro caso la VM Debian - si posiziona tra due comunicanti legittimi - nel nostro caso la VM Kali Linux e il gateway - e ne intercetta tutto il traffico.

La corretta configurazione e l'utilizzo di **Ettercap** mi ha consentito di intercettare tutto il traffico della VM Kali Linux. A conferma di questo allego un'immagine catturata dalla VM Debian, che mostra come sono
~~~

riuscito a catturare dei fittizi dati di login inseriti dall'utilizzatore della VM Kali Linux su una pagina HTTP visitata.



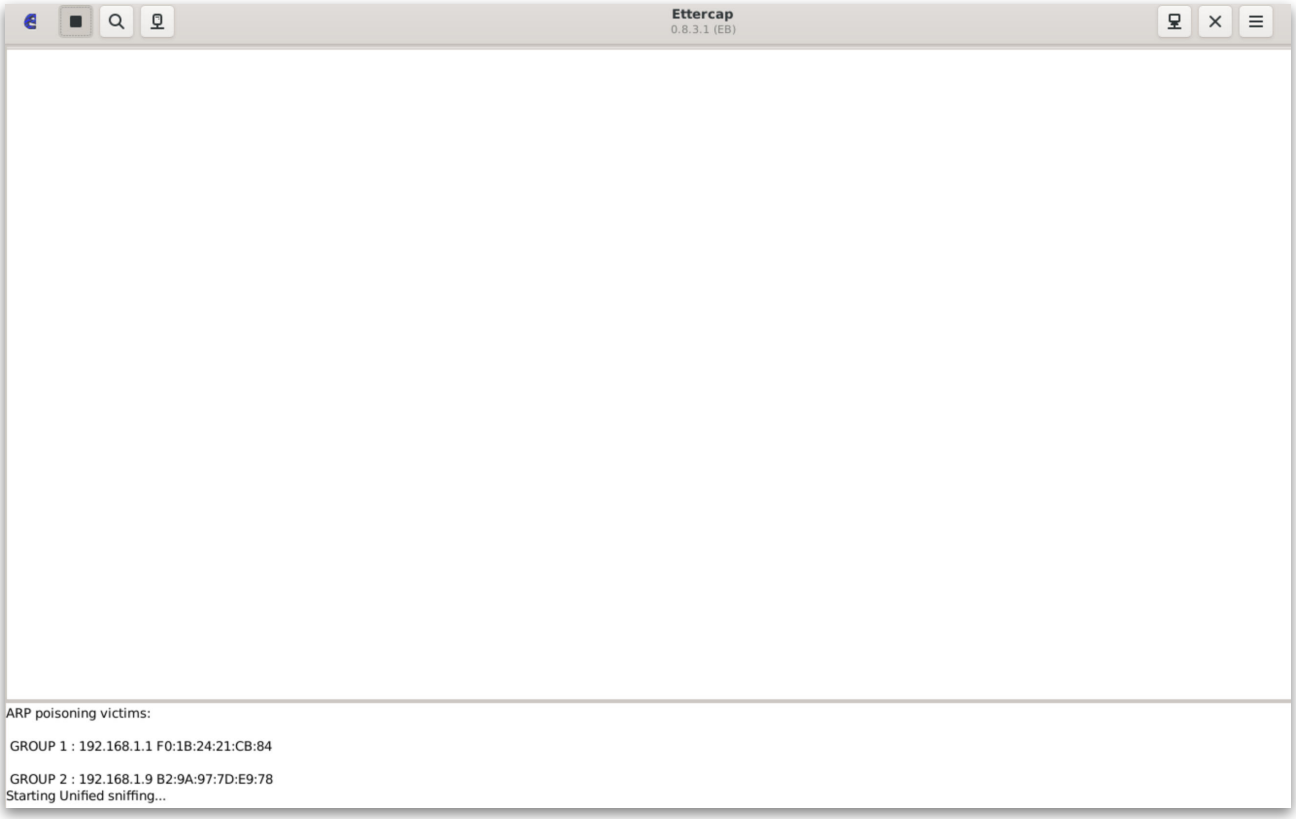
~~~

ANNOTAZIONI TECNICHE

L'attacco **Man-in-the-Middle** (MITM) è una forma di intercettazione in cui un attaccante si posiziona in modo furtivo tra due parti che comunicano legittimamente, intercettando o alterando i dati scambiati senza che le vittime se ne accorgano. L'obiettivo principale è la compromissione della riservatezza e dell'integrità della comunicazione. In alcuni casi, come quello dell'esercizio, è possibile intercettare anche i dati di login.

Quando si parla di reti LAN, una delle tecniche più comuni per realizzare un attacco di questo tipo è **l'ARP Poisoning**. Questa tecnica sfrutta una vulnerabilità del protocollo ARP (Address Resolution Protocol), utilizzato per mappare gli indirizzi IP agli indirizzi MAC all'interno di una rete locale. Semplificando, l'attaccante invia dei messaggi ARP falsificati così che la vittima pensi che il MAC dell'attaccante sia quello legittimo del gateway e che il gateway, a sua volta, pensi che il MAC dell'attaccante sia quello legittimo della vittima. Tramite questo espediente, tutto il traffico fra le due parti viene intercettato dall'attaccante, posizionato in mezzo (in-the-Middle) fra le due macchine.

Per simulare un attacco Man-in-the-Middle, ho messo sulla stessa rete una VM Debian (la macchina attaccante) e una VM Kali Linux (la macchina target). Gli indirizzi IP delle due macchine sono **192.168.1.7** per la Debian e **192.168.1.9** per la Kali Linux. Entrambe le VM sono configurate per utilizzare il gateway 192.168.1.1, ed entrambe possono uscire su Internet grazie all'utilizzo del DHCP.

Il primo passo è stato quello di installare Ettercap su Debian, visto che non è fra i tool pre-installati. Il processo prevede prima l'installazione delle componenti del programma, poi l'installazione dell'interfaccia grafica. Il comando utilizzato è:
~~~

sudo apt install ettercap-common ettercap-graphical

Un punto fondamentale dell'esercizio è quello di abilitare l'IP Forwarding. Questa funzionalità permette a un dispositivo di fungere da router, consentendogli quindi di ricevere pacchetti IP destinati a indirizzi non propri e di inoltrarli verso la loro destinazione finale attraverso l'interfaccia di rete appropriata. Nel caso in oggetto, l'abilitazione dell'IP Forwarding ha consentito il corretto smistamento di tutti i pacchetti. Il comando (da eseguire sulla VM Debian attaccante) è:

sudo sysctl -w net.ipv4.ip_forward=1

Completate queste operazioni, ho avviato Ettercap con il comando **sudo ettercap -G**. Questo mi ha consentito di utilizzare l'interfaccia grafica. Una volta avviato il programma, ho eseguito la scansione degli hosts per individuare la VM Kali Linux (la macchina target) e il Gateway. Una volta identificati e segnalati come target, ho poi selezionato il tipo di attacco, scegliendo **ARP poisoning** dall'apposito menù MITM. Da questo momento, Ettercap ha cominciato a inviare i pacchetti ARP falsificati al Gateway e alla VM Kali Linux, in modo da reindirizzare il loro traffico alla VM Debian (la macchina attaccante).



Per comprovare l'effettiva riuscita dell'attacco Man-in-the-Middle, l'esercizio richiedeva di raggiungere dalla macchina target un particolare sito HTTP (http://testphp.vulnweb.com/login.php) e **simulare l'immissione di un nome utente e una password**. Come mostra lo screenshot allegato al paragrafo SOLUZIONE, i fittizi dati di login immessi dall'utilizzatore della VM Kali Linux (la macchina target) sono stati intercettati da Ettercap in esecuzione sulla VM Debian (la macchina attaccante). Questa è la dimostrazione che l'attacco Man-in-the-Middle in ambiente simulato è andato a buon fine.