INDICE

PRIMA PARTE

NULL SESSION: è una connessione anonima a un servizio di rete, tipicamente SMB su sistemi Windows, che consente l'accesso a determinate informazioni senza fornire credenziali di autenticazione.
Storicamente, questo comportamento era previsto per motivi di compatibilità e amministrazione remota, ma si è rivelato una grave debolezza di sicurezza in quanto permette a un attaccante di interrogare il sistema ottenendo informazioni sensibili come utenti, gruppi, condivisioni di rete e policy di sicurezza, senza alcuna autorizzazione.
In pratica, la Null Session sfrutta una configurazione permissiva del servizio SMB che accetta connessioni con username e password vuoti, consentendo una forma di enumerazione non autenticata.

SISTEMI VULNERABILI A NULL SESSION: sistemi storicamente vulnerabili alle Null Session includono:
1. Windows NT 4.0
2. Windows 2000
3. Windows XP
4. Windows Server 2000 e 2003

Questi sistemi permettevano, di default o tramite configurazioni deboli, l'accesso anonimo a risorse SMB.
Ad oggi, questi sistemi non sono più supportati né sicuri, ma il rischio rimane concreto in ambienti legacy, reti industriali, laboratori, infrastrutture obsolete o sistemi non aggiornati.
I sistemi Windows moderni (Windows 10, 11, Windows Server recenti) non sono vulnerabili di default, ma possono diventarlo in caso di:
- configurazioni errate,
- downgrade delle policy di sicurezza,
- utilizzo di SMBv1,
- ambienti Active Directory mal configurati.

MITIGAZIONE: la vulnerabilità può essere mitigata o eliminata adottando le seguenti misure:
- Disabilitare l'accesso anonimo ai servizi SMB
- Disabilitare SMBv1, protocollo obsoleto e insicuro
- Applicare policy di sicurezza restrittive sull'accesso alle risorse di rete
- Limitare l'enumerazione di utenti e gruppi solo a utenti autenticati
- Mantenere i sistemi aggiornati con patch di sicurezza
- Isolare i sistemi legacy in reti segmentate e controllate

Queste misure riducono la superficie di attacco legata all'accesso anonimo.

ARP POISONING: l'ARP Poisoning (o ARP Spoofing) è una tecnica di attacco che sfrutta il funzionamento del protocollo ARP utilizzato per associare indirizzi IP a indirizzi MAC all'interno di una rete locale.
Poiché ARP non prevede meccanismi di autenticazione un attaccante può inviare messaggi ARP falsificati alla rete, inducendo due host legittimi a credere che l'indirizzo MAC dell'attaccante corrisponda all'IP dell'altro host.
In questo modo, il traffico di rete viene deviato attraverso la macchina dell'attaccante, che può intercettare, analizzare o modificare i pacchetti scambiati, realizzando un attacco Man-in-the-Middle.

SISTEMI VULNERABILI ALL' ARP POISONING: sono vulnerabili ad ARP Poisoning tutti i sistemi che utilizzano ARP in reti locali, in assenza di protezioni specifiche.
In particolare:
- Sistemi Windows
- Sistemi Linux
- Sistemi macOS
- Dispositivi embedded e IoT
- Router e switch non gestiti
- Reti Wi-Fi e LAN non protette

La vulnerabilità non dipende dal sistema operativo in sé, ma dall'assenza di controlli sul protocollo ARP all'interno della rete.

MITIGAZIONE, RILEVAMENTO E PREVENZIONE ARP POISONING:

PREVENZIONE

La prevenzione dell'ARP Poisoning consiste nell'evitare che un attaccante possa introdurre associazioni IP–MAC false all'interno della rete e si basa su controlli di rete e configurazioni difensive.

Le principali misure preventive includono:

- Dynamic ARP Inspection (DAI) sugli switch gestiti, che verifica la validità dei messaggi ARP confrontandoli con una tabella DHCP affidabile,
- Segmentazione della rete tramite VLAN, riducendo il numero di host che condividono lo stesso dominio di broadcast,
- Disabilitazione o limitazione delle porte non utilizzate sugli switch,
- Utilizzo di ARP statici per host critici (gateway, server), soluzione efficace ma poco scalabile,
- Preferire reti cablate o Wi-Fi protette rispetto a reti aperte o non controllate.

RILEVAMENTO

Il rilevamento dell'ARP Poisoning ha l'obiettivo di individuare anomalie nel traffico ARP che possano indicare la presenza di un attacco in corso.

I principali segnali e tecniche di rilevamento sono:

- Cambiamenti frequenti o sospetti nelle tabelle ARP (stesso IP associato a MAC diversi)
- Presenza di ARP reply non richiesti (gratuitous ARP anomali)
- Monitoraggio del traffico ARP tramite strumenti di analisi di rete o IDS
- Utilizzo di software di sicurezza in grado di rilevare conflitti IP–MAC
- Analisi di rallentamenti o interruzioni anomale della comunicazione di rete

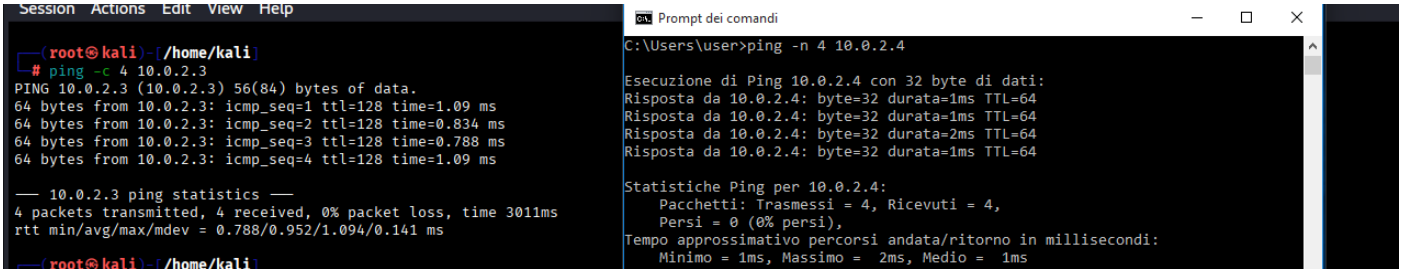
MITIGAZIONE

La mitigazione riguarda le azioni da intraprendere una volta che l'attacco è stato individuato, con l'obiettivo di ripristinare il corretto funzionamento della rete e ridurre i danni.

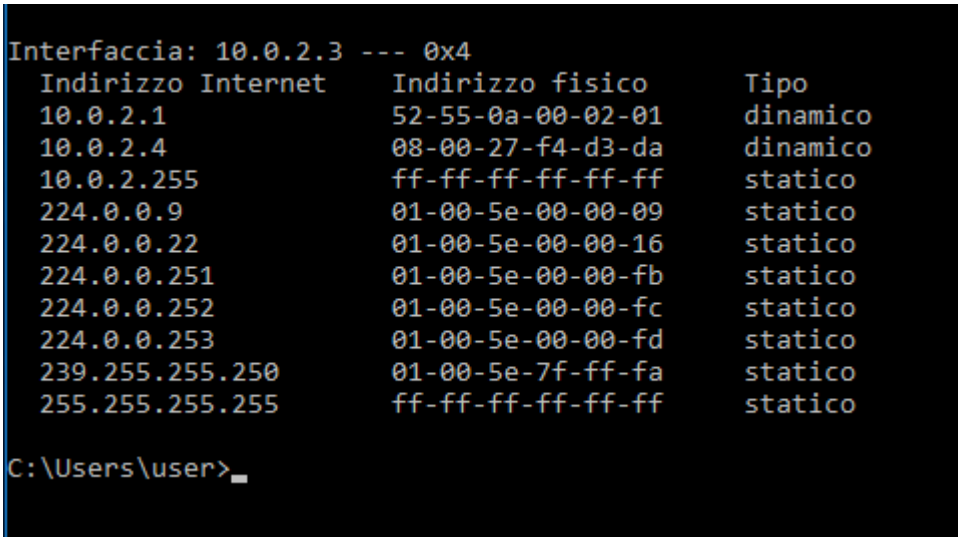
Le principali azioni di mitigazione includono:

- Interruzione immediata dell'attacco, isolando il dispositivo sospetto dalla rete
- Ripristino delle associazioni ARP corrette (svuotamento cache ARP o reinserimento manuale)
- Forzare l'uso di protocolli cifrati (HTTPS, TLS, SSH) per impedire la lettura dei dati intercettati
- Analisi del traffico catturato per valutare l'eventuale esposizione di credenziali o dati sensibili
- Rafforzamento delle misure preventive per evitare il ripetersi dell'attacco.

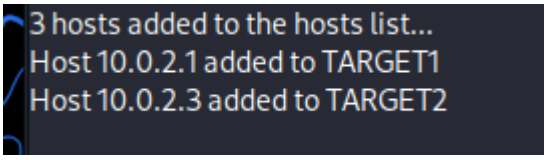
SECONDA PARTE



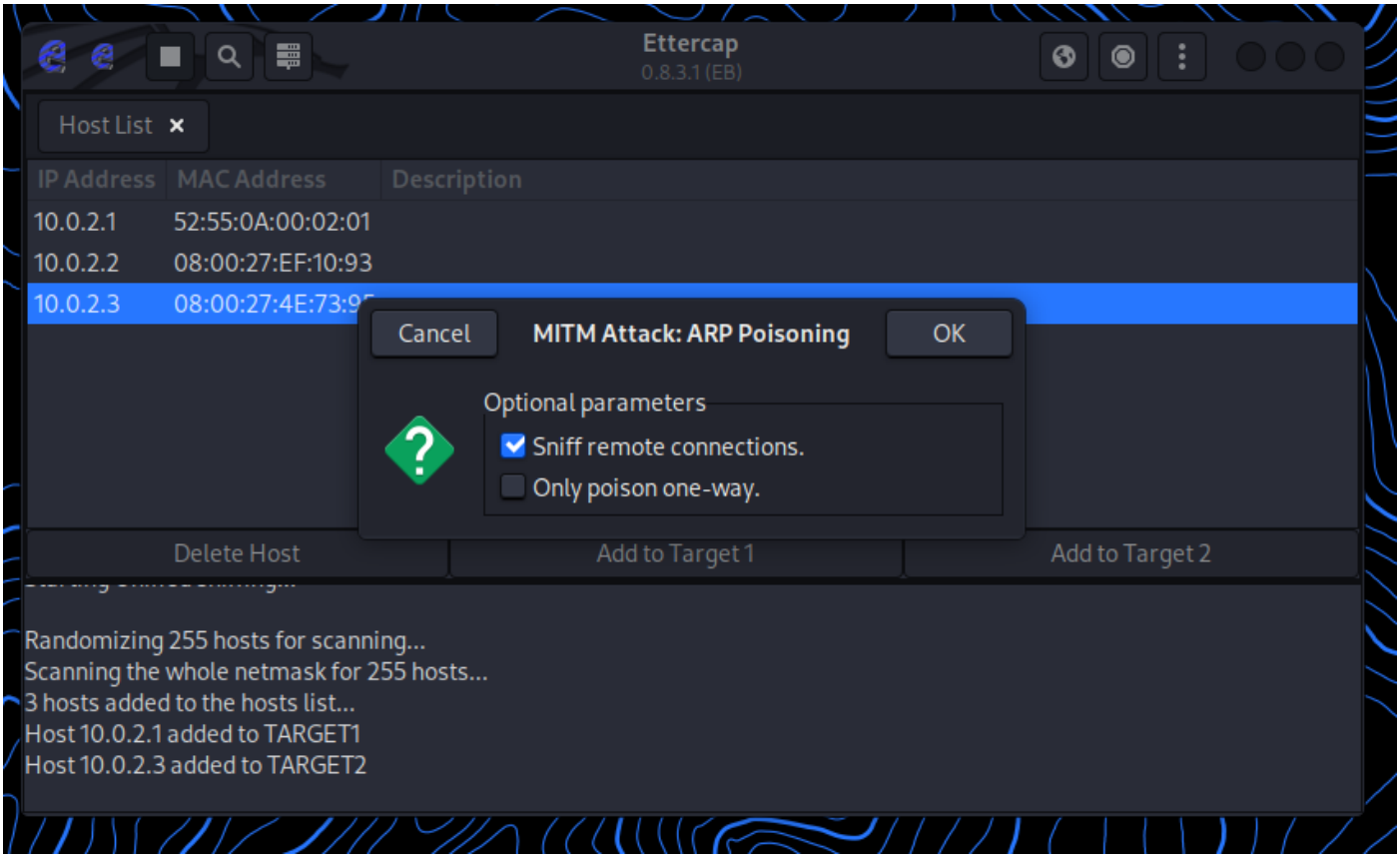
In questa fase è stata verificata la presenza di connettività tra le due macchine coinvolte nel laboratorio al fine di confermare che potessero comunicare correttamente all'interno dello stesso contesto di rete.
La verifica ha evidenziato che la comunicazione tra i sistemi è attiva e bidirezionale, condizione necessaria per poter osservare e analizzare il traffico generato durante le fasi successive dell'esercizio.



In questa fase è stata osservata la tabella ARP del sistema Windows per documentare lo stato iniziale delle associazioni tra indirizzi IP e indirizzi MAC presenti nella rete.
L'analisi mostra una situazione coerente con il normale funzionamento del protocollo ARP, in cui ogni indirizzo IP risulta associato al corretto indirizzo MAC del dispositivo corrispondente.
In particolare, l'indirizzo IP del gateway è associato al proprio indirizzo MAC legittimo, mentre gli altri host presenti nella rete mantengono associazioni univoche e stabili.
Le informazioni raccolte verranno utilizzate come termine di confronto per evidenziare le modifiche introdotte successivamente, quando verranno applicate tecniche di interferenza sul traffico di rete e alterate deliberatamente le associazioni IP–MAC.



Ettercap è stato impiegato come piattaforma di analisi e manipolazione del traffico in rete locale, consentendo di posizionare il sistema Kali in una posizione intermedia tra i dispositivi coinvolti nella comunicazione.
In questa fase sono stati individuati e selezionati i due host di interesse: da un lato il gateway di rete e dall'altro il sistema Windows; tali host sono stati assegnati rispettivamente ai due gruppi di target previsti dallo strumento, definendo in modo esplicito le estremità della comunicazione che si intende osservare e influenzare.
La selezione dei target ha lo scopo di preparare l'ambiente per l'intervento attivo sulla rete, permettendo a Kali di presentarsi come intermediario tra il sistema vittima e il gateway.
In questo modo, il traffico scambiato tra i due host può essere intercettato e analizzato, senza interrompere la comunicazione apparente tra le parti.

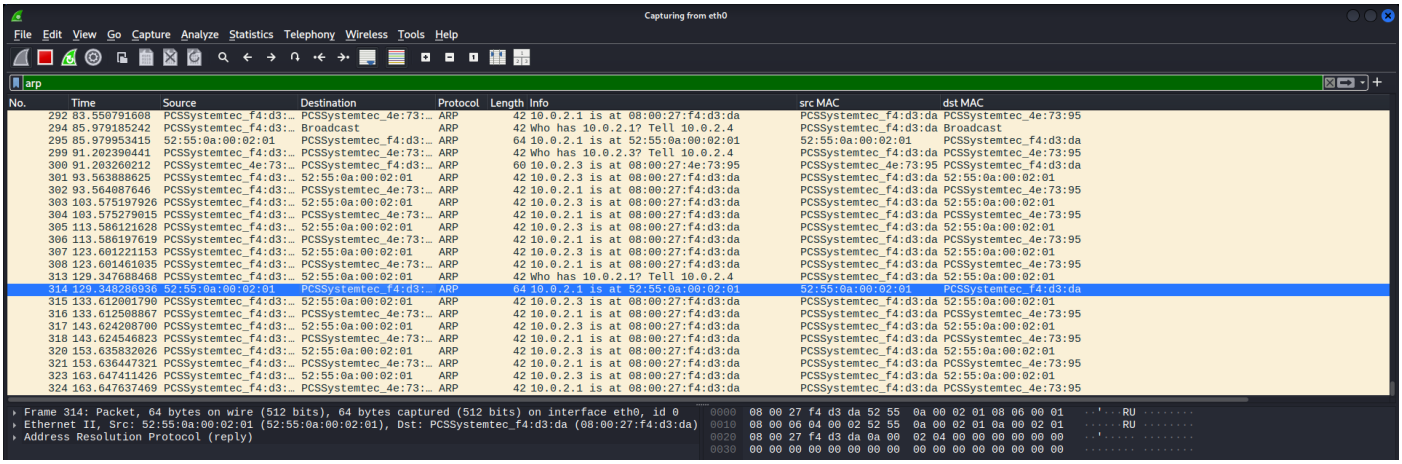


Una volta completata la fase di preparazione e definiti i target di interesse, è stato avviato l'attacco di tipo ARP Poisoning tramite Ettercap.
Con questa operazione il sistema Kali viene inserito attivamente nel flusso di comunicazione tra il sistema Windows e il gateway di rete, assumendo il ruolo di intermediario senza interrompere la normale operatività percepita dagli host coinvolti.
L'attivazione dell'attacco consente di inviare risposte ARP alterate ai dispositivi target, inducendoli ad associare l'indirizzo IP del gateway e quello del sistema vittima all'indirizzo MAC di Kali; in questo modo, il traffico destinato a uno dei due host viene instradato attraverso il sistema attaccante, che può così osservare e analizzare le comunicazioni in transito.
In questa fase non si riscontrano interruzioni evidenti del servizio né anomalie percepibili dal punto di vista dell'utente finale quindi la rete continua a funzionare apparentemente in modo regolare, mentre a livello logico vengono introdotte modifiche che alterano il percorso effettivo dei pacchetti.
L'avvio dell'ARP Poisoning rappresenta il punto di svolta del laboratorio svolto , poiché da questo momento le associazioni IP–MAC presenti nella rete non riflettono più lo stato iniziale documentato, ma vengono deliberatamente manipolate per consentire l'intercettazione del traffico.

```
C:\Users\user>arp -a

Interfaccia: 10.0.2.3 --- 0x4
  Indirizzo Internet    Indirizzo fisico      Tipo
  10.0.2.1              08-00-27-f4-d3-da     dinamico
  10.0.2.2              08-00-27-ef-10-93     dinamico
  10.0.2.4              08-00-27-f4-d3-da     dinamico
  10.0.2.255            ff-ff-ff-ff-ff-ff     statico
  224.0.0.9             01-00-5e-00-00-09     statico
  224.0.0.22            01-00-5e-00-00-16     statico
  224.0.0.251           01-00-5e-00-00-fb     statico
  224.0.0.252           01-00-5e-00-00-fc     statico
  224.0.0.253           01-00-5e-00-00-fd     statico
  239.255.255.250       01-00-5e-7f-ff-fa     statico
  255.255.255.255       ff-ff-ff-ff-ff-ff     statico

C:\Users\user>
```

```
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.4  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::efdd:5149:9431:335b  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:f4:d3:da  txqueuelen 1000  (Ethernet)
        RX packets 200  bytes 23344 (22.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 350  bytes 24244 (23.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 10  bytes 580 (580.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10  bytes 580 (580.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Confrontando lo stato della rete prima e dopo l'intervento, emerge una differenza chiara e nel modo in cui vengono risolte le associazioni tra indirizzi IP e indirizzi MAC.
In una condizione iniziale di funzionamento normale, ogni host presente nella rete locale risulta correttamente associato al proprio indirizzo fisico: ciascun indirizzo IP viene risolto verso il MAC reale del dispositivo destinatario, consentendo una comunicazione diretta e trasparente tra i nodi della rete.
Successivamente all'intervento, la situazione risulta modificata in modo evidente, ossia l'analisi delle tabelle ARP mostra indirizzi IP, precedentemente associati a dispositivi distinti, risultano ora mappati sullo stesso indirizzo MAC, appartenente alla macchina Kali.
Questo cambiamento indica che le risposte ARP non riflettono più la reale topologia fisica della rete, ma presentano informazioni alterate che inducono i sistemi a inoltrare il traffico verso un host intermedio; la comunicazione continua a funzionare correttamente dal punto di vista degli endpoint, ma il percorso dei pacchetti non è più diretto: il traffico viene intercettato e ritrasmesso senza che l'utente finale percepisca anomalie operative.



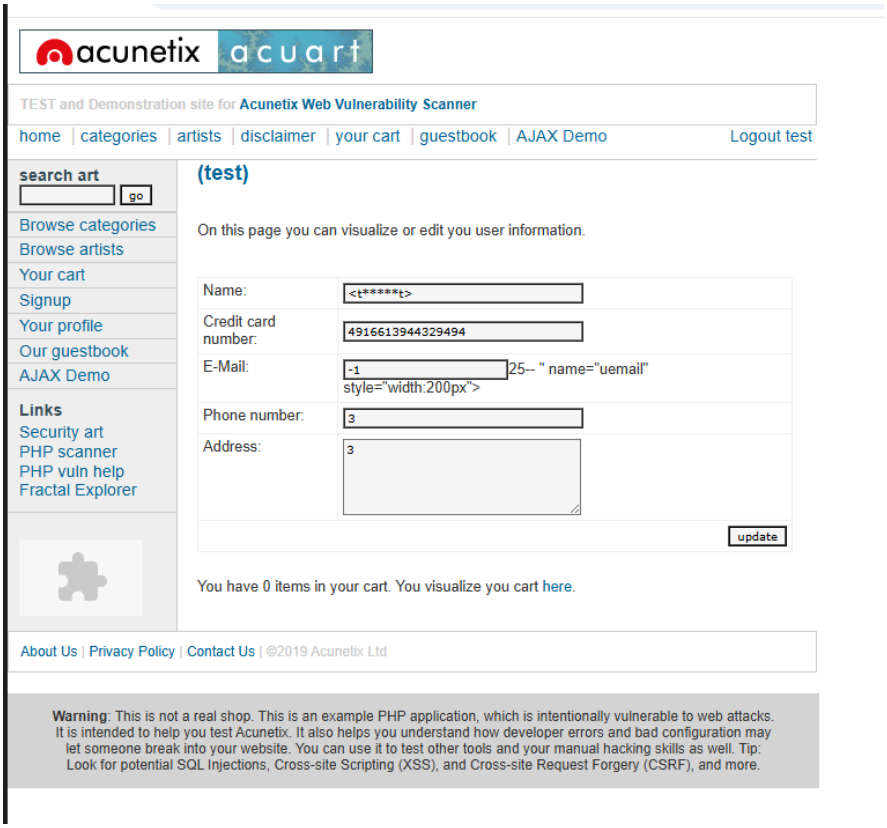
L’analisi del traffico in Wireshark mostra chiaramente una variazione rispetto alla situazione iniziale della rete.

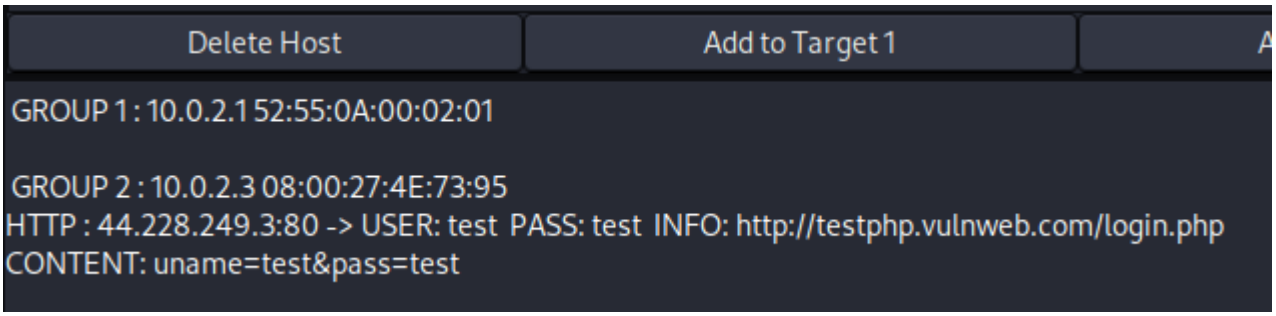
Sono visibili numerosi pacchetti ARP di risposta ripetuti nel tempo, nei quali lo stesso indirizzo MAC viene associato a più indirizzi IP; in condizioni normali questo comportamento non si verifica, poiché le associazioni IP-MAC sono stabili e aggiornate solo quando necessario.

La presenza di risposte ARP continue e non richieste indica che un nodo sta forzando l’aggiornamento delle tabelle ARP degli altri sistemi e di conseguenza, il traffico destinato ai diversi host viene temporaneamente indirizzato verso un punto intermedio, che assume un ruolo centrale nello scambio dei dati senza interrompere la comunicazione.

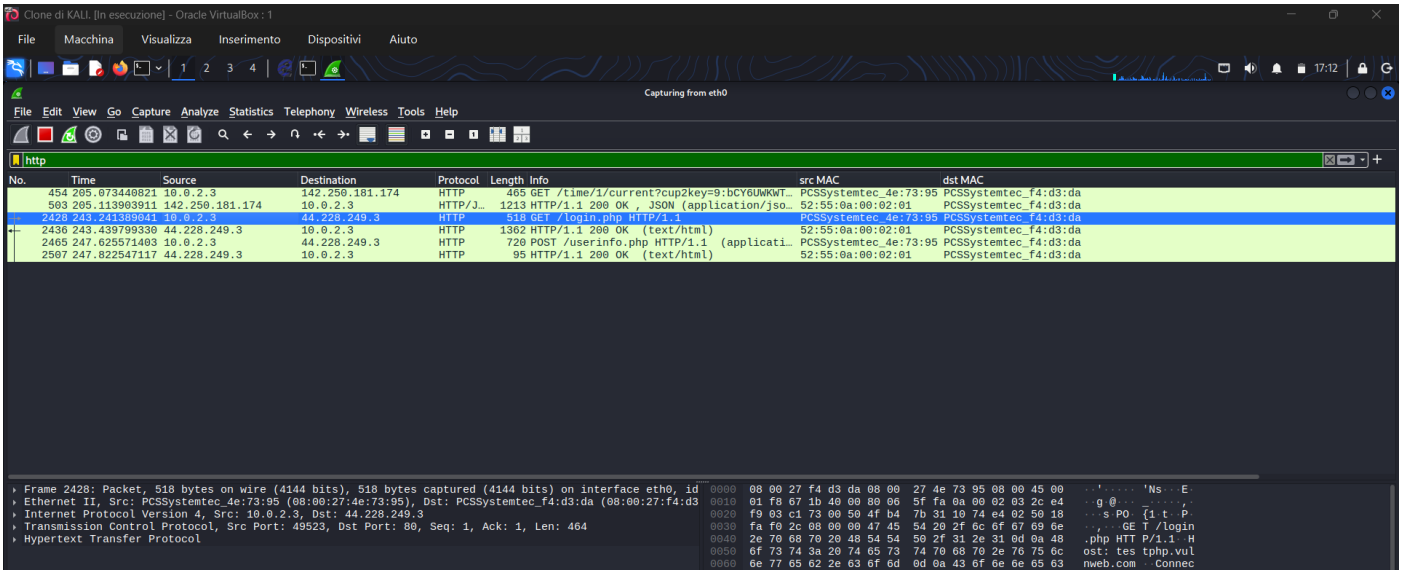
Questa evidenza conferma il cambiamento dello stato della rete e dimostra come la risoluzione ARP, da meccanismo di supporto, venga sfruttata per influenzare il percorso del traffico.

A seguito dell'alterazione delle associazioni ARP e del posizionamento del sistema Kali come nodo intermedio nella comunicazione, è stato possibile osservare il traffico applicativo generato dalla macchina vittima durante la normale navigazione web.
Poiché la comunicazione avviene tramite protocollo HTTP non cifrato, le informazioni trasmesse tra client e server risultano leggibili lungo il percorso di rete.
La sessione di autenticazione, pur avvenendo correttamente dal punto di vista dell'utente finale, espone in chiaro i parametri inviati al server, inclusi i dati di login e le informazioni inserite nei campi del profilo utente. Questo comportamento evidenzia come, in assenza di meccanismi di cifratura del traffico, un attore posizionato all'interno del flusso di rete possa intercettare contenuti sensibili senza alterare il funzionamento dell'applicazione né generare anomalie percepibili dall'utente.
L'evidenza raccolta dimostra in modo concreto l'impatto combinato di una debolezza a livello di rete (ARP Poisoning) e di una comunicazione applicativa non protetta. Anche in presenza di sistemi funzionanti e apparentemente sicuri, l'assenza di cifratura espone dati critici a intercettazione passiva, con potenziali conseguenze rilevanti in contesti aziendali, regolamentati o ad alta criticità informativa.





Al termine del laboratorio è stato eseguito un attacco di tipo Man-In-The-Middle utilizzando Ettercap, con l'obiettivo di intercettare il traffico HTTP generato da un utente durante l'accesso a un'applicazione web vulnerabile.
Attraverso l'ARP Poisoning, Ettercap si è posizionato logicamente tra la macchina della vittima e il gateway di rete, consentendo all'attaccante di osservare il traffico in transito senza interrompere la comunicazione né generare anomalie percepibili dall'utente.
Una volta avviata la sessione MITM, l'utente ha effettuato l'accesso all'applicazione web tramite browser, utilizzando una normale pagina di login raggiungibile in http; poiché il protocollo HTTP non prevede cifratura dei dati, le informazioni di autenticazione sono state trasmesse in chiaro sulla rete , ettercap ha intercettato tali richieste e ha reso immediatamente visibili lo username e la password inseriti dall'utente, mostrando in modo esplicito i parametri della richiesta HTTP contenenti le credenziali.



L’analisi del traffico tramite Wireshark conferma l’effettiva riuscita dell’attacco Man-In-The-Middle.

Durante la sessione MITM, il traffico HTTP generato dalla vittima viene intercettato e ispezionato in tempo reale; in particolare, è possibile osservare la richiesta HTTP di tipo GET /login.php diretta al server remoto, seguita dalla richiesta POST contenente i dati di autenticazione.

Poiché la comunicazione avviene su protocollo HTTP non cifrato, le informazioni sensibili risultano immediatamente leggibili all’interno del payload del pacchetto. Questo dimostra in modo inequivocabile come l’attaccante, pur non interagendo direttamente con l’applicazione web, sia in grado di acquisire credenziali valide semplicemente intercettando il traffico di rete, sfruttando la posizione di intermediario ottenuta tramite ARP Poisoning.

CONCLUSIONE

Il laboratorio ha mostrato in modo pratico come un attacco Man-In-The-Middle basato su ARP Poisoning consenta a un attaccante di intercettare il traffico di rete senza interrompere la comunicazione tra client e server.

Una volta posizionato come intermediario, l'attaccante è in grado di osservare le richieste HTTP generate dall'utente e leggere in chiaro le informazioni trasmesse.

Nel caso analizzato, l'accesso a un'applicazione web non cifrata ha permesso di visualizzare direttamente username e password durante la fase di autenticazione. L'utente non riceve alcun segnale evidente dell'attacco e il servizio continua a funzionare normalmente, rendendo la compromissione difficile da individuare senza strumenti di monitoraggio dedicati.

L'attività evidenzia quindi come l'assenza di cifratura del traffico renda inefficaci molte difese applicative e come un attacco MITM possa compromettere la riservatezza delle credenziali anche in assenza di vulnerabilità dirette sul server.