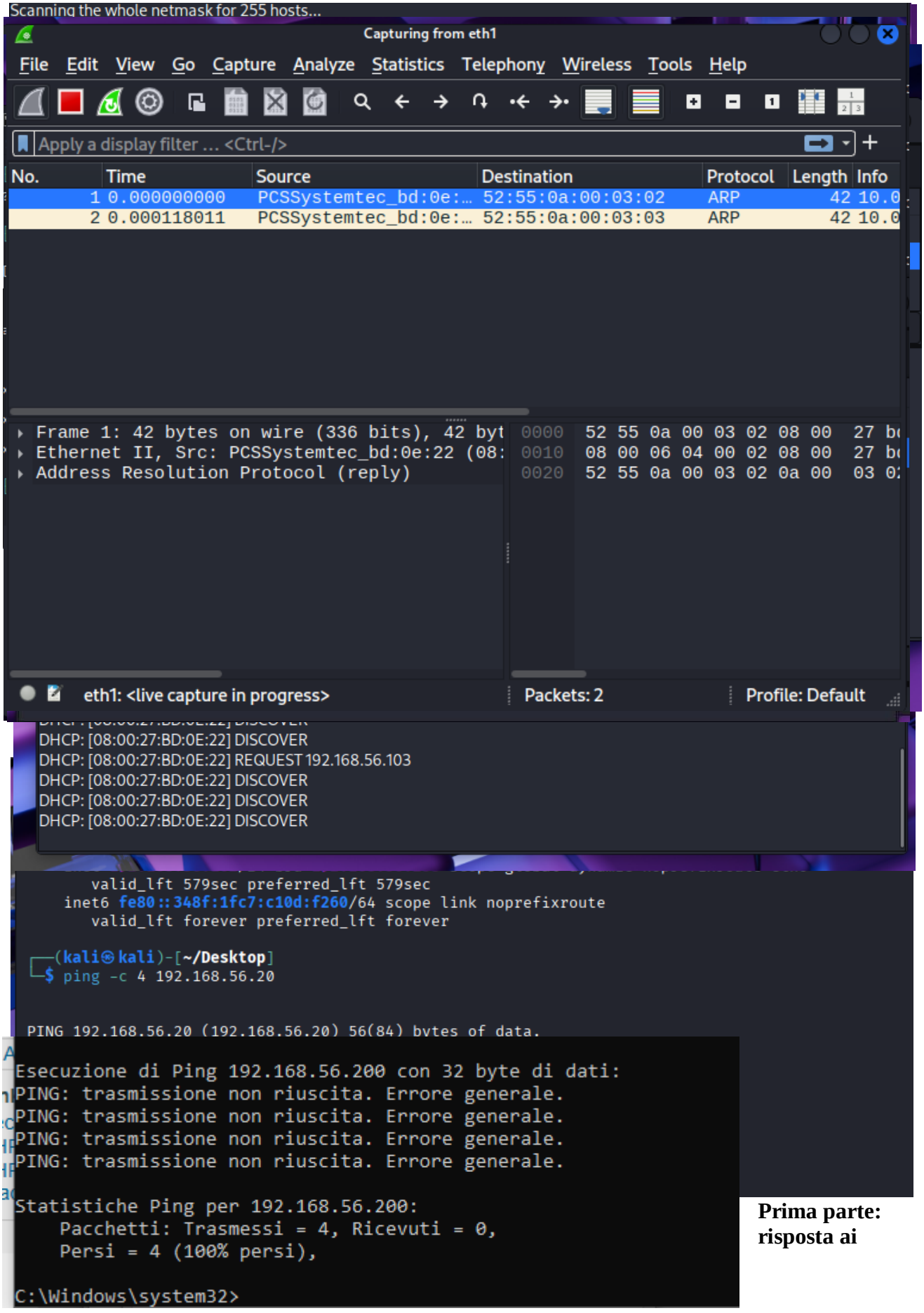
W15D1- FRANCESCO MONTALTO



Prima parte: risposta ai

quesiti:

1) Spiegare brevemente cosa vuol dire Null Session

Una Null Session è una connessione anonima a un sistema Windows che non richiede nome utente né password. Avviene tramite il servizio SMB (che sta per "Server Message Block") e l' IPC$ (che sta per "Inter-Process Communication Share), quest'ultimo utilizzato per far comunicare processi e computer in rete.

Tramite questa falla (perché di questo parliamo) un attaccante può collegarsi alla condivisione "\\nomehost\IPC$" senza autenticazione, potendo così ottenere informazioni sensibili come nomi utenti e gruppi di dominio, condivisioni di rete, policy di sicurezza, nomi delle macchine nel dominio e addirittura dati su servizi e permessi.

2) Elencare i sistemi che sono vulnerabili a Null Session e se sono ancora in commercio

-WINDOWS NT / WINDOWS 2000: Storicamente vulnerabili alle Null Session in un'epoca in cui la cybersicurezza non era sviluppata. Non sono più venduti, chiaramente.

-WINDOWS SERVER 2008 / 2008 R2: Hanno restrizioni migliori rispetto ai predecessori, ma ci sono delle modalità di configurazione dove attacchi anonimi possono persistere se mal configurati. Non sono più disponibili, in larga scala.

-WINDOWS MODERNI (7,8,10,11, SERVER 2012/2016/2019/2022): Non consentono normalmente Null Session anonime per le operazioni che sfruttavano SMB/IPC$, ma ci sono delle eccezioni, come meccanismi di retrocompatibilità che possono riaprire la porta, o controller di dominio che possono esporre alcune pipe RPC accessibili a utenti anonimi di alcune configurazioni. Le RPC permettono a un programma di eseguire una funzione in un altro spazio di indirizzamento, inclusa un'altra macchina.
Queste versioni sono ancora oggi in commercio e in uso, ma più che nella versione pura la vulnerabilità è un fatto di configurazione.

-SAMBA: Samba, se correttamente configurato, può consentire accessi anonimi simili a null session; vecchie distribuzioni o settaggi di retrocompatibilità possono esporre la stessa superfice di attacco. E' attualmente ancora in commercio e molto diffuso.

-FIRMWARE CHE IMPLEMENTANO SMB:
I firmware che implementano SMB (Server Message Block) sono utilizzati principalmente nei dispositivi di archiviazione di rete (NAS) e nei router, come i prodotti di Synology e Western Digital, per consentire la condivisione di file, stampanti e altre risorse con i computer Windows. Il servizio SMB è un protocollo di rete utilizzato principalmente per la condivisione di file, stampanti e altre risorse tra computer in una rete locale. Permette a un computer di accedere a file e cartelle su un altro computer della rete come se fossero locali, facilitando la collaborazione e l'accesso centralizzato ai dati.
Sono attualmente sul mercato; molti dispositivi consumer e industriali usano SMB e possono essere mal configurati.

3) Elencare le modalità per mitigare o risolvere la vulnerabilità Null Session

Azioni immediate di mitigazione:

1) Disabilitazione dell'accesso anonimo / null session a livello Windows, tramite GPO o registry. Le impostazioni di sicurezza in GPO sono il metodo raccomandato, in particolare per limitare l'accesso anonimo alle condivisioni e ai named pipe e per negare l'autorizzazione "Everyone" per gli utenti anonimi. Altrimenti, su registry, tramite l'editor del sistema (regedit.exe) si naviga fino alla chiave "parameters" e si crea o modifica il valore DWORD "RestrictNullSessAccess" Si imposta il valore su 1 per disabilitare l'accesso anonimo.

2) Si disabilita SMB v1 dal pannello di controllo (dal momento che, evidentemente, presenta alcune lacune di sicurezza. In particolare, è necessario creare regole sui firewall o sulle liste di controllo degli accessi (ACL) per negare tutto il traffico sulle porte TCP/UDP 139 e 445, specialmente ai confini della rete (perimeter) e tra i segmenti di rete interni. Questa operazione impedisce la comunicazione non autorizzata per la condivisione di file, stampanti e altre risorse.

3) Si verifica e si corregge la configurazione Samba con "restrict anonymous = 2". Poi, si modifica il file di configurazione "smb.conf" su Linux/NAS, posizionando la direttiva restrict anonymous = 2 nel file corretto, solitamente sotto la sezione "global" e poi riavviare il servizio Samba. La direttiva "restrict anonymous = 2" imposta le opzioni di autenticazione, ma l'esatto comportamento e la configurazione corretta possono variare a seconda del sistema operativo e della versione di Samba.

4) Si verifica l'esito della mitigazione con "enum4linux" (questo strumento serve per testare se il target accetta ancora connessioni SMB anonime) con il comando base
"enum4linux -a <IP_Target>"
o con gli script NSE di nmap, tramite il comando base
"nmap -p 139,445 --script smb-enum-shares,smb-enum-users <IP_Target>"
Sulla base dei risultati,
-se ci sono output con nomi utenti, share o info di dominio = vulnerabilità ancora attiva.
-se gli script riportano "access denied" o "no share found" = mitigazione efficace.

4) Spiegare brevemente come funziona l'ARP Poisoning

L'Arp poisoning è un tipo di attacco informatico che sfrutta la semplicità "ingenua" del protocollo Arp. Il protocollo ARP (Address Resolution Protocol) è utilizzato dai dispositivi di una rete per associare un indirizzo IP (livello di rete) all'indirizzo MAC (Media Access Control, livello di

collegamento) corrispondente.
Quando un dispositivo vuole contattarne un altro sulla stessa rete, fa la richiesta, in soldoni, "di chi è questo IP?" e si fida della prima risposta ricevuta che, qualora fosse di un attaccante, potrebbe essere una risposta Arp falsa che comunica "sono io quell'IP", con il relativo MAC. Così le macchine vittima aggiornano la loro ARP cache e cominciano a inviare il traffico destinato al gateway o a un host sensibile direttamente all'attaccante che, una volta in mezzo, può ispezionare, modificare o bloccare i pacchetti andando da semplice e fastidioso **sniffer** (un programma o dispositivo che cattura il traffico di rete mentre passa da un computer all'altro) a completo **man-in-the-middle** (attacco in cui l'aggressore si inserisce tra due soggetti che credono di comunicare direttamente tra loro).

5) Elencare i sistemi che sono vulnerabili a ARP Poisoning

Bene o male qualsiasi dispositivo IPv4 nello stesso dominio di broadcast può essere preso di mira, perché l'Arp funziona solo dentro un dominio di broadcast, cioè dentro la stessa rete locale (LAN). Ma alcuni sono molto più appetibili per un attaccante. Vediamo quali:

-Postazioni client (Windows, Linux, macOS) su LAN non protette

-Server locali (file server, domain controller, gateway) se non isolati in VLAN

-Dispositivi IoT e smart (telecamere, sensori, smart-TV, stampanti di rete)

-Switch non gestiti e hub

-Switch gestiti mal configurati (se manca la configurazione sono inutili)

-Client su reti Wi-Fi aperte

-Virtual machine e container sulla stessa bridge/host (per lo stesso motivo: il traffico resta nello stesso dominio di broadcast virtuale)

-Dispositivi di rete legacy o industriali, che spesso usano protocolli non cifrati e sono difficili da aggiornare

-NAS e dispositivi di storage in LAN che espongono interfacce di amministrazione o condivisioni non protette. I NAS (Network Attached Storage) sono dispositivi di archiviazione collegati alla rete, progettati per condividere file tra più utenti o sistemi

-Endpoint BYOD e dispositivi personali degli utenti: possono essere compromessi e usati per avvelenare la LAN. Gli endpoint BYOD (Bring Your Own Device) sono i dispositivi personali che gli utenti portano e usano dentro una rete aziendale o scolastica: laptop, smartphone, tablet, a volte persino smartwatch.

-Gateway e router di piccola impresa/consumer se esposti sulla LAN interna senza protezioni

5) Elencare le modalità per mitigare, rilevare o annullare l'ARP Poisoning

Possiamo dividere questa operazione in tre fasi: mitigazione, rilevazione, annullamento.

Mitigazione: Le misure di mitigazione servono a ridurre la possibilità che un attacco ARP Poisoning vada a buon fine.

In primis, bisogna inserire manualmente le associazioni IP–MAC per i dispositivi più importanti, come router, server o gateway. E' abbastanza efficace in reti piccole. Su Linux, un esempio può essere "arp -s 192.168.1.1 00:11:22:33:44:55"

E' opportuno anche separare la rete in più VLAN, in quanto limita la propagazione di un eventuale attacco: un ARP poisoning in una VLAN non influenza le altre.

La Dynamic ARP Inspection (DAI)
è una funzionalità disponibile su molti switch gestiti.
Confronta i pacchetti ARP con la tabella DHCP e scarta quelli sospetti o non validi.
È una delle misure più efficaci in ambiente aziendale. Come detto, lavora in combinazione con DHCP Snooping, che registra le associazioni IP-MAC create dal server DHCP e aiuta a individuare host falsi o non autorizzati.

E' utile anche limitare il numero di indirizzi MAC ammessi su una singola porta di rete, riducendo la possibilità che un attaccante cambi continuamente identità.

Rilevazione*:* Per riconoscere un ARP Poisoning è possibile monitorare la rete o analizzare le tabelle ARP.

In primis, è opportuno un controllo manuale della tabella ARP, tramite il comando
"arp -a". Se lo stesso MAC address compare associato a più indirizzi IP, è probabile che sia in corso un attacco. E' utile anche utilizzare strumenti di monitoraggio, come Wireshark, che come sappiamo permette di osservare il traffico di rete e individuare pacchetti ARP falsi.

Dopo un'analisi del traffico anomalo, è possibile stabilire la diagnosi. Un numero elevato di pacchetti ARP gratuiti ("who-has") o continui aggiornamenti sospetti può indicare un avvelenamento.

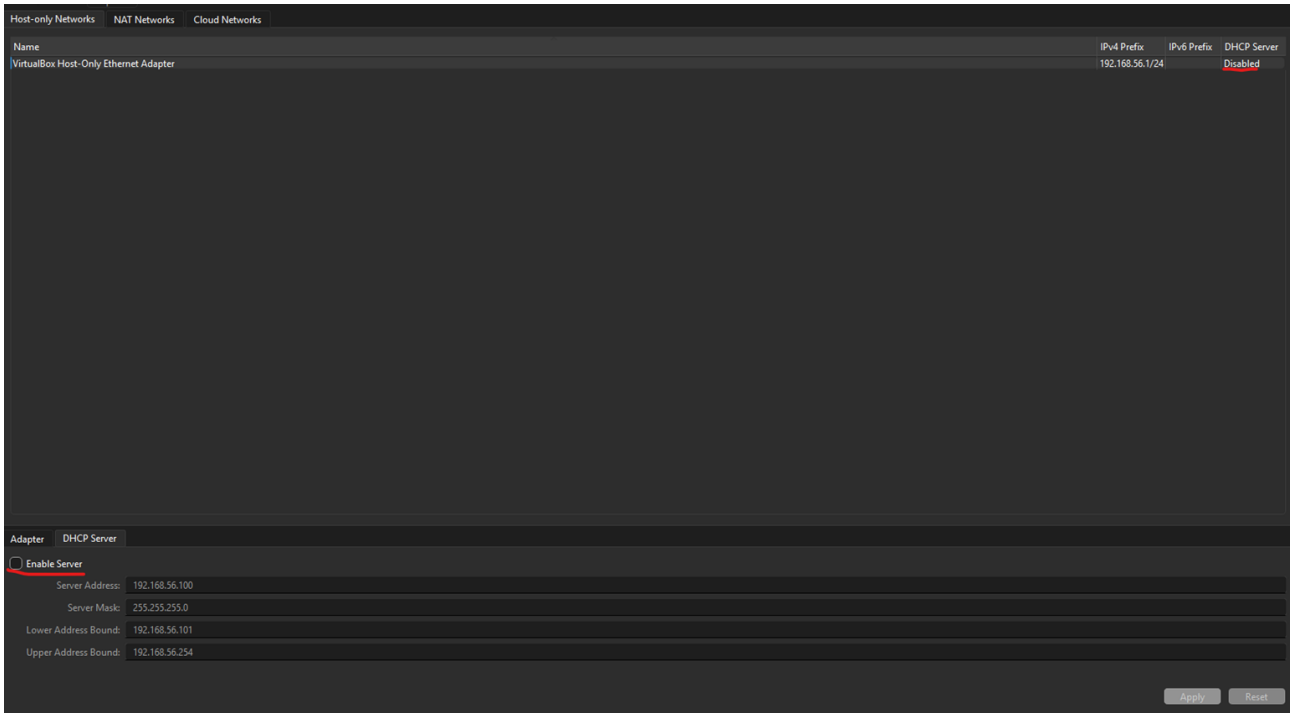
Annullamento*:* In caso di avvelenamento ARP già in corso, si possono adottare le seguenti contromisure.
1. Pulizia della cache ARP (flush): cancella tutte le associazioni ARP memorizzate. Si effettua tramite il comando "ip -s -s neigh flush all" o "arp -d *" su Windows.

2.Dopo la pulizia, è possibile reinserire manualmente le voci IP–MAC sicure tramite ARP statico.

3.In caso di tabelle corrotte, è utile riavviare router e switch per svuotare completamente la memoria ARP.

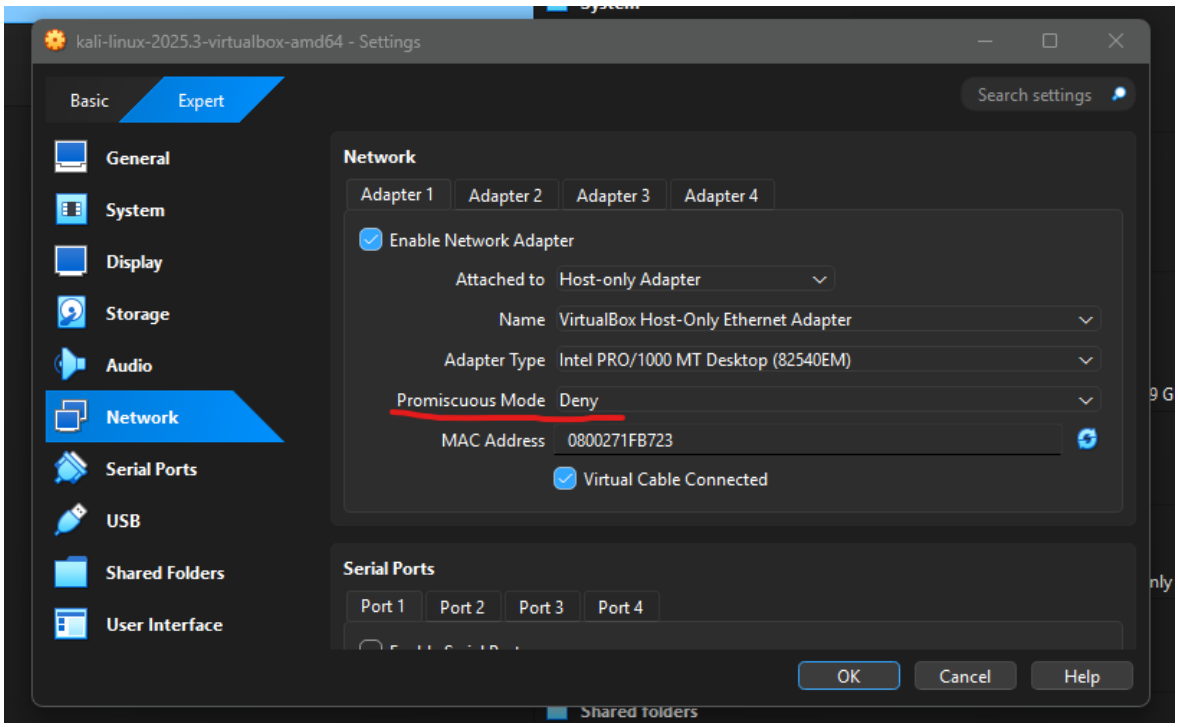
4. È possibile bloccare il dispositivo malevolo tramite firewall o switch:
"iptables -A INPUT -m mac --mac-source XX:XX:XX:XX:XX:XX -j DROP"
Seconda parte: Esercizio guidato su Ettercap.

1. Avvio le due VM su una stessa rete virtuale isolata (host-only / internal) che ho modificato sulla voce "Network" , in cui mi sono assicurato che DPCH fosse disattivo.

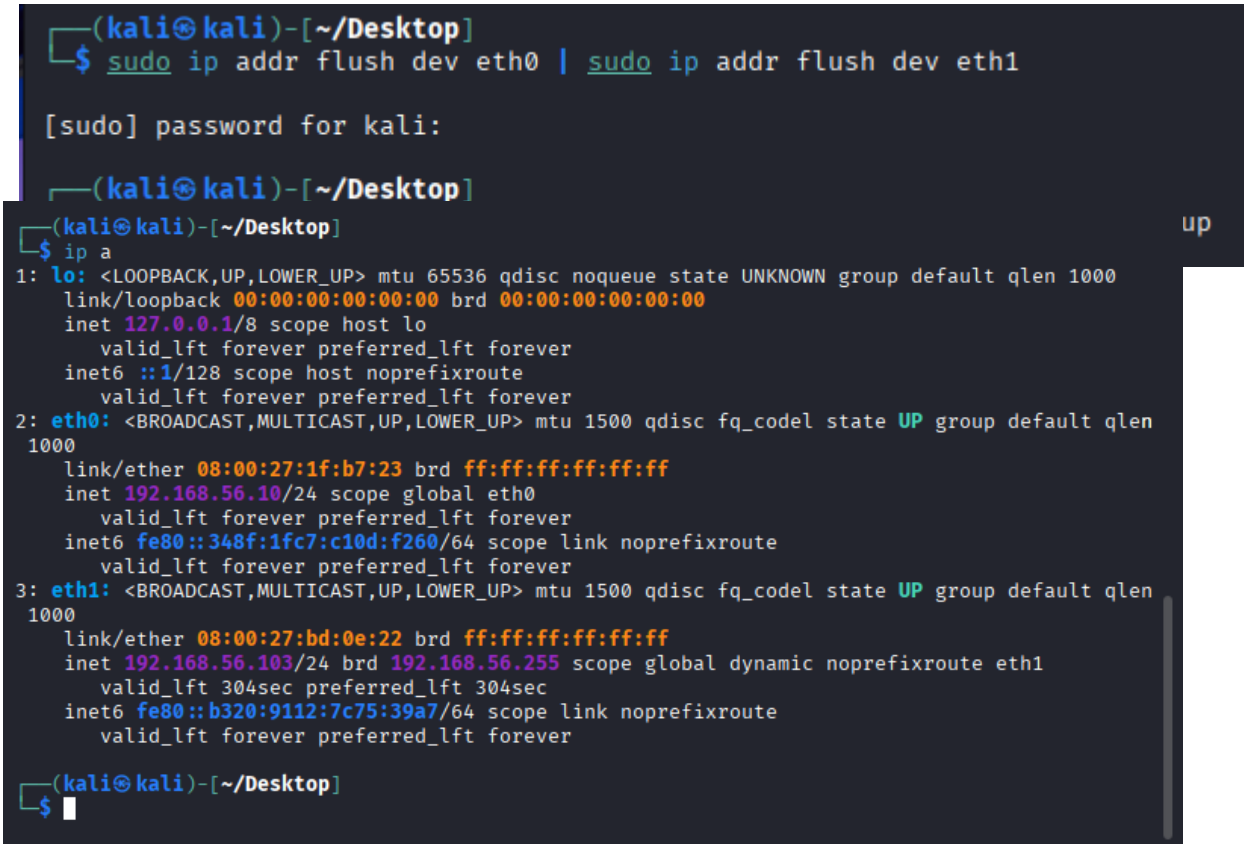


Un DHCP attivo può riallocare indirizzi ad ogni boot, causando collisioni o cambiamenti imprevisti che invalidano i risultati del test.

Mi sono anche assicurato che la “Promiscuous Mode” fosse settata su “Deny”, perché in promiscuous mode la scheda passa al sistema operativo tutti i frame che vede sul bus virtuale, non solo quelli indirizzati al suo MAC. Questo serve per sniffare il traffico di altri host sulla stessa LAN virtuale.


kali-linux-2025.3-virtualbox-amd64 - Settings
Basic
Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to
Host-only Adapter
Name
VirtualBox Host-Only Ethernet Adapter
Adapter Type
Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode
Deny
MAC Address
0800271FB723
Virtual Cable Connected
Serial Ports
Port 1
Port 2
Port 3
Port 4
OK
Cancel
Help

2. Dopo una verifica con “ip a”, ho rimosso gli IP correnti da entrambe le interfacce, ed ho impostato la mia Kali con “eth0” con inet 192.168.56.10/24. Poi c’è un’altra interfaccia eth1 con 192.168.56.103/24.



3. Ho successivamente impostato l'IP sulla macchina vittima (Metasploitable, ovviamente).

4. Ho eseguito dei controlli rapidi verso la macchina vittima per verificarne la connettività, affinché potessi avviare tranquillamente Ettercap. La connettività ha dato esito positivo.

5. Ho poi, finalmente, avviato Ettercap.

Ed ho eseguito "Scans for host" per far partire la scansione degli host che ho nella mia rete.

Mi sono poi assicurato che la vittima fosse attiva (nel mio caso: 192.168.56.20 e che il gateway presente nella Hosts list.

7. **Ho controllato con “arp -a”.**

Come visibile, Kali vede correttamente Metasploitable a livello di rete e link .

8. Ho assegnato i target giusti ai due dispositivi

Rispettivamente “target 1” e “target 2”

9. Ho fatto partire l’attacco con “arp poisoning”

Ho quindi atteso l’eventuale riuscita.

10. Ho verificato sulla macchina vittima se l'attacco fosse riuscito effettivamente.
Risposta affermativa.

Come visibile, entrambi gli IP puntano allo stesso MAC, ossia quello della mia Kali.
Metasploitable pensa che Kali sia il gateway (192.168.56.1)
E ovviamente pensa anche che Kali sia Kali; quindi qualsiasi pacchetto destinato al gateway passa ora da Kali.

Ho quindi proceduto a "sniffare" le credenziali.

11. Ho quindi aperto Wireshark

Ho scelto eth0 e filtrato per “arp”

12. Prove visuali:

Sono visibili due dispositivi diversi:
con stesso MAC address eaventi il mio MAC, indice del fatto che tutti i pacchetti passano per me

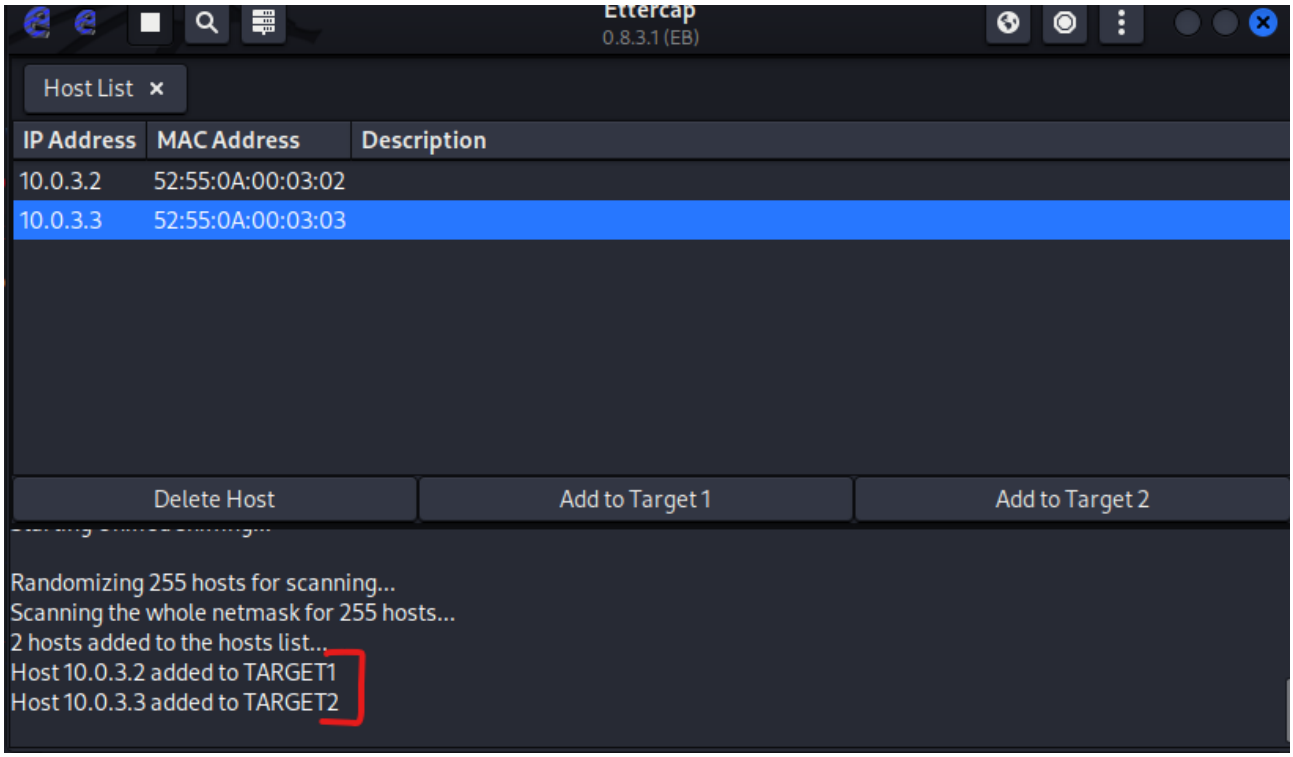
È la prova schiacciante che:

Ci troviamo ufficialmente in mezzo (Man-In-The-Middle)

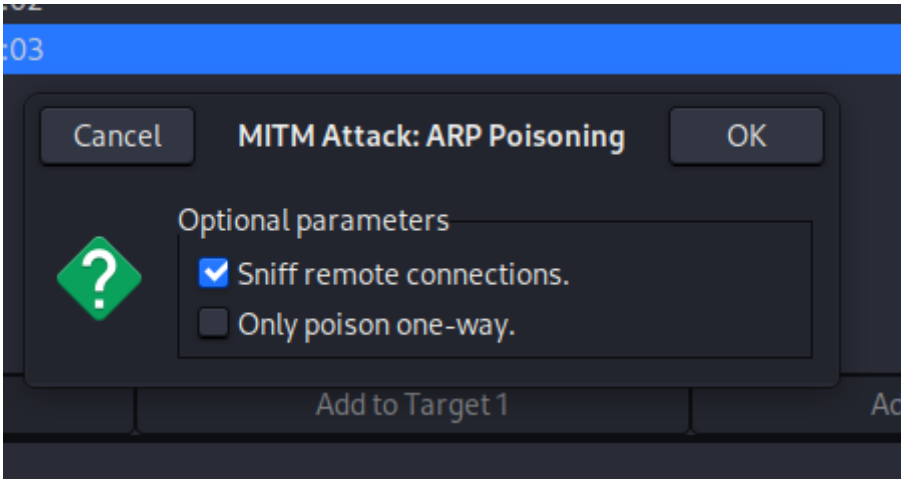
Questi pacchetti che possiamo osservare sono risposte ARP della tua Kali, inviate direttamente alla vittima.

13. Ho aperto e attivato Ettercap

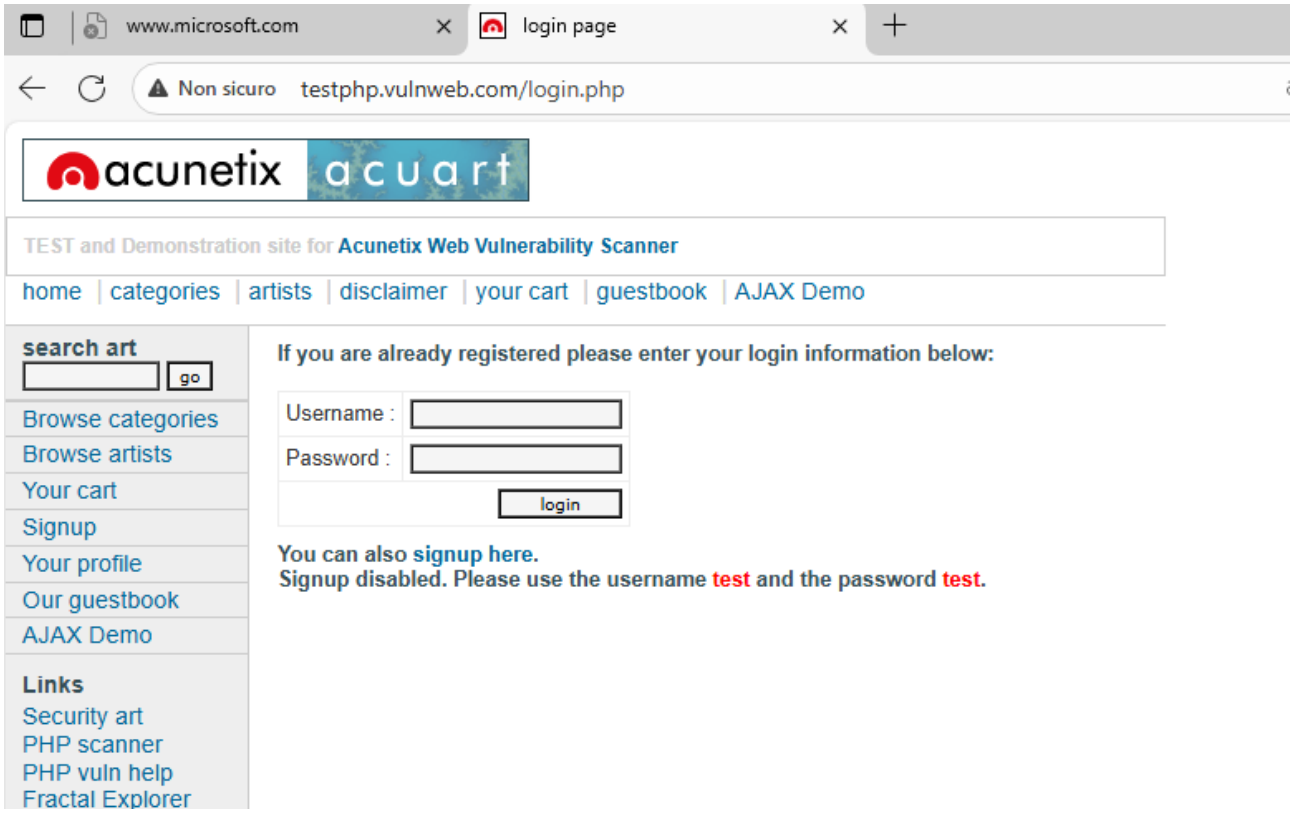
14. Prima di attivare il test, ho attivato i rispettivi target.



E ho poi attivato “arp poisoning”…



15. Sono poi andato sul browser della mia VM Windows 10 nella page di login di VulnWeb.



Ho quindi digitato due credenziali a caso (ma a cui dovrò prestare attenzione, per verificarle successivamente) e ho premuto “Login”

16. Ho aperto WireShark per intercettare il traffico, assicurandomi di star sniffando sulla scheda giusta.

Problema riscontrato:

Nonostante la corretta configurazione degli strumenti di analisi, nell'atto ho riscontrato una criticità strutturale dovuta alla modalità di virtualizzazione della rete. Le interfacce delle VM si trovavano su segmenti differenti (NAT, Host-Only) e non condividendo lo stesso broadcast domain non è stato possibile generare correttamente traffico ARP verso l'host vittima, ricevere le risposte ARP necessarie ad avviare l'attacco MITM e inoltrare il traffico IP tra le macchine virtuali in maniera trasparente.

ESERCIZIO FACOLTATIVO:

Per le Null Session, la soluzione migliore da utilizzare è bloccare l'accesso anonimo alle condivisioni. Questa cosa funziona bene, perché chi prova ad entrare senza password non riesce più a vedere utenti, cartelle e informazioni del sistema. L'utente normale non si accorge di niente, continua ad usare il computer come sempre. Per l'azienda non è un grande lavoro, basta impostarlo una volta e vale per tutti i PC.
Per l'ARP Poisoning le difese sono più complicate. Una cosa che aiuta tanto è usare sempre siti HTTPS, così anche se qualcuno si mette in mezzo alla rete non può leggere la password. Oppure bisogna configurare meglio gli switch e la rete per bloccare i pacchetti falsi. Anche qui per l'utente non cambia nulla, però per l'azienda serve più lavoro e magari anche dispositivi migliori.