EPICODE

ESERCIZIO W15D1

NULL SESSION e ARP POISONING

Mungiovì Fabio

TASK

PRIMA PARTE

Rispondere ai seguenti quesiti:

- Spiegare brevemente cosa vuol dire Null Session
- Elencare i sistemi che sono vulnerabili a Null Session e se sono ancora in commercio
- Elencare le modalità per mitigare o risolvere la vulnerabilità Null Session
- Spiegare brevemente come funziona l'ARP Poisoning
- Elencare i sistemi che sono vulnerabili a ARP Poisoning
- Elencare le modalità per mitigare, rilevare o annullare l'ARP Poisoning

Facoltativo

Commentare le azioni di mitigazione scelte, spiegando l'efficacia e l'effort per l'utente e per l'azienda.

SECONDA PARTE

Esercizio guidato su Ettercap

Configuriamo un attacco di ARP poisoning per intercettare le comunicazioni tra i sistemi Windows 7 e Metasplotable

ESECUZIONE

PRIMA PARTE

Null Session

La "Null Session" è una connessione di rete che un computer può stabilire con un server Windows senza bisogno di credenziali (nome utente o password).
Permetteva di ottenere informazioni sul sistema, come nomi di utenti, risorse condivise e dettagli sul sistema operativo.

Sistemi vulnerabili e se sono ancora in commercio:

Questa vulnerabilità ha riguardato principalmente sistemi operativi Microsoft Windows più datati, in particolare Windows NT, Windows 2000, Windows XP e Windows Server 2003.
Questi sistemi non sono più in commercio o, se lo sono, non sono supportati ufficialmente da Microsoft.
Pertanto, la vulnerabilità Null Session è ormai considerata obsoleta per i sistemi moderni.

Modalità per mitigare o risolvere la vulnerabilità Null Session:

La soluzione principale è stata implementata da Microsoft con le versioni successive di Windows.
Per i sistemi più vecchi, si potevano applicare le seguenti misure:

- **Disabilitare il servizio "Server" o "NetBIOS su TCP/IP":**
  Questo impediva le connessioni Null Session.
- **Configurare le autorizzazioni:**
  Restringere l'accesso anonimo alle risorse condivise e alle informazioni del sistema.
- **Applicare le patch di sicurezza:**
  Microsoft ha rilasciato aggiornamenti che hanno chiuso questa falla.

ARP Poisoning

L'ARP Poisoning (o ARP Spoofing) è una tecnica con cui un attaccante inganna i dispositivi su una rete locale (LAN) per farli credere che il suo indirizzo MAC sia quello del router (gateway) o di un altro computer.
In pratica, l'attaccante invia messaggi ARP falsi che associano il suo indirizzo MAC all'indirizzo IP del gateway.
Così, tutto il traffico destinato al gateway passerà attraverso l'attaccante, che può leggerlo, modificarlo o bloccarlo.

Sistemi vulnerabili a ARP Poisoning:

L'ARP Poisoning non è una vulnerabilità di un sistema operativo specifico, ma piuttosto un punto debole del protocollo ARP stesso, che è fondamentale per il funzionamento delle reti locali.
Pertanto, tutti i dispositivi connessi a una rete locale che si basano sul protocollo ARP sono potenzialmente vulnerabili.

Modalità per mitigare, rilevare o annullare l'ARP Poisoning:

- **ARP statico:**
  Configurare manualmente le voci ARP sui dispositivi critici per associare un indirizzo IP a un indirizzo MAC specifico, impedendo così modifiche non autorizzate. (Soluzione efficace ma non scalabile per grandi reti).
- **Software di rilevamento ARP Spoofing**:
  Utilizzare strumenti che monitorano il traffico ARP alla ricerca di anomalie o messaggi ARP duplicati o sospetti.

- **Sicurezza delle porte switch (Port Security):**
  Configurare gli switch di rete per limitare gli indirizzi MAC consentiti su ciascuna porta, impedendo a un attaccante di spacciarsi per un altro dispositivo.
- **DHCP Snooping:**
  Configurare gli switch di rete per fidarsi solo dei messaggi DHCP da fonti autorizzate, aiutando a prevenire la manipolazione degli indirizzi IP e MAC.
- **Crittografia (es. HTTPS, VPN):**
  Anche se l'ARP Poisoning può reindirizzare il traffico, la crittografia end-to-end protegge i dati rendendoli illeggibili all'attaccante.

Facoltativo (Commento alle azioni di mitigazione)

Null Session

- Applicare le patch di sicurezza e aggiornare i sistemi operativi:
  - Efficacia: Altissima.
    È la soluzione più efficace perché chiude direttamente la vulnerabilità a livello di sistema operativo.
  - Effort utente: Basso.
    Si tratta di abilitare gli aggiornamenti automatici o installare le patch quando disponibili, un'azione comune nella manutenzione dei sistemi.
  - Effort azienda: Basso-Medio.
    Richiede una politica di aggiornamento costante e, in alcuni casi, test per assicurarsi che gli aggiornamenti non creino problemi di compatibilità con software legacy. Tuttavia, è un costo necessario per la sicurezza.

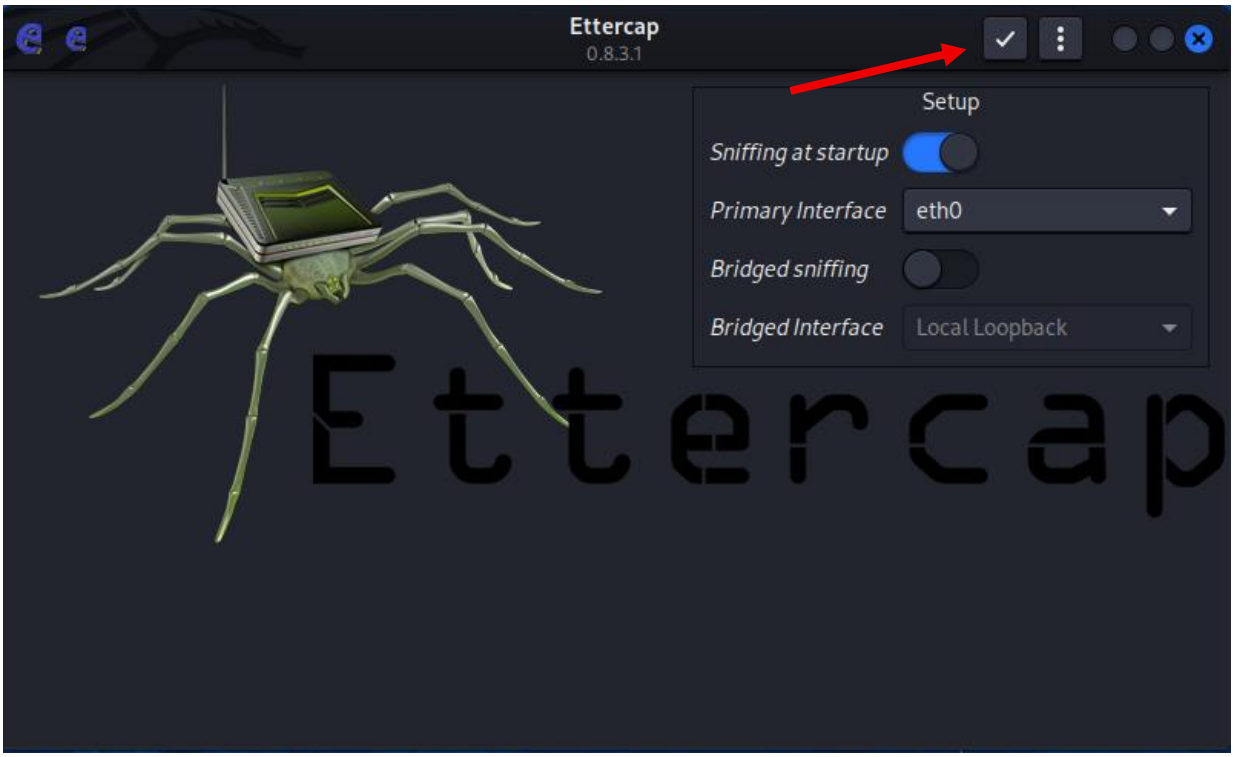
ARP Poisoning

- Crittografia (HTTPS, VPN):
  - Efficacia: Molto alta per la protezione dei dati.
    Anche se l'attaccante intercetta il traffico, non può decifrarlo.
  - Effort utente: Basso.
    L'utente naviga su siti HTTPS o usa una VPN senza particolari accorgimenti una volta configurata.
  - Effort azienda: Medio-Alto.
    Per l'HTTPS, le aziende devono implementare certificati SSL/TLS sui propri server web. Per le VPN, devono configurare e mantenere l'infrastruttura VPN. È un investimento significativo ma cruciale per la privacy e l'integrità dei dati.
- Sicurezza delle porte switch (Port Security) e DHCP Snooping:
  - Efficacia: Alta.
    Soprattutto per prevenire attacchi all'interno della rete locale.
    Rendono molto più difficile per un attaccante ingannare i dispositivi.
  - Effort utente: Nessuno.
    Queste configurazioni sono trasparenti per l'utente finale.
  - Effort azienda: Medio-Alto.
    Richiede personale IT qualificato per configurare correttamente gli switch di rete. È un investimento in infrastruttura e competenze, ma migliora drasticamente la sicurezza della rete interna.

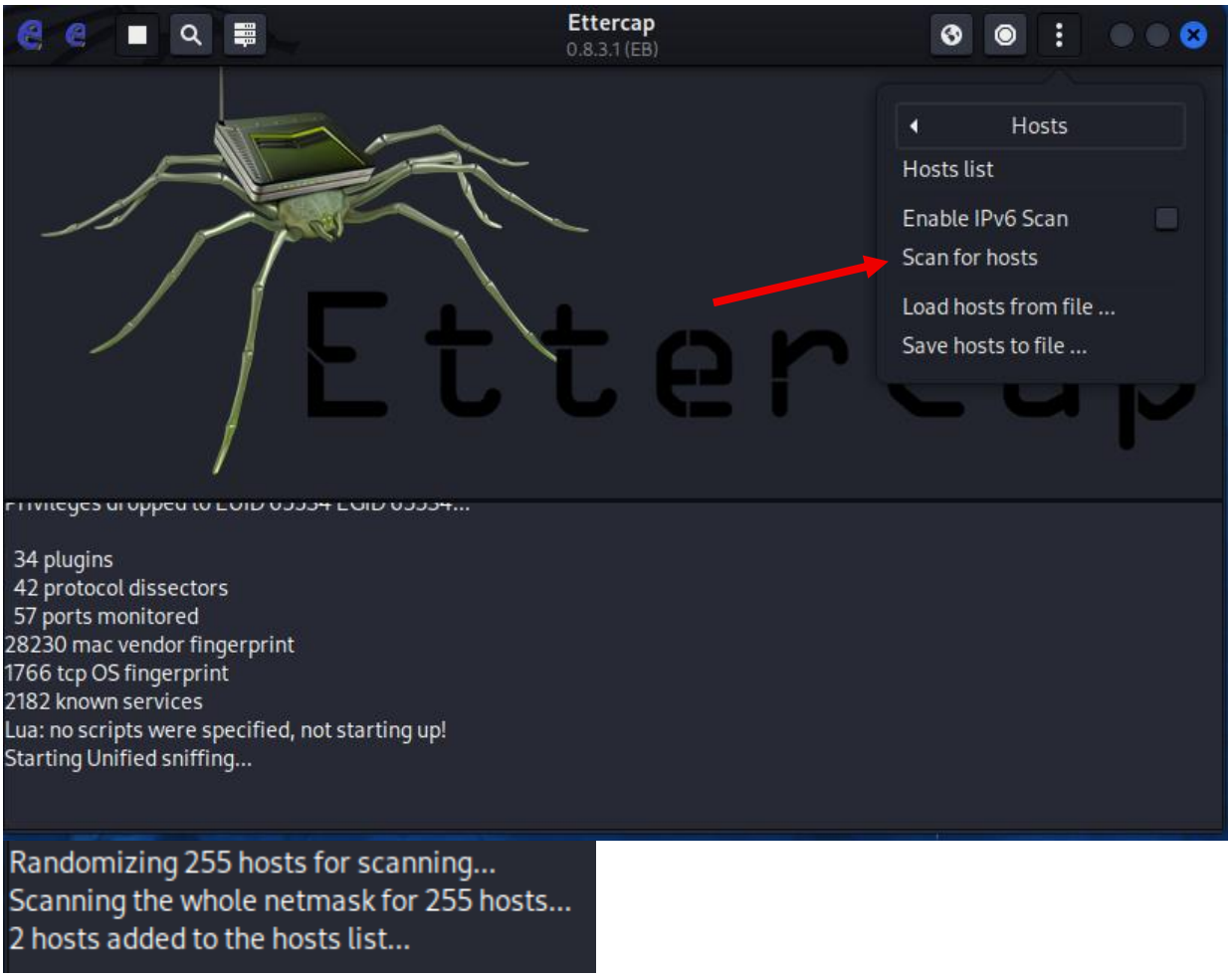
SECONDA PARTE

Per questa esercitazione iniziamo aprendo la GUI di Ettercap.

Clicchiamo sulla spunta per avviare il tool.

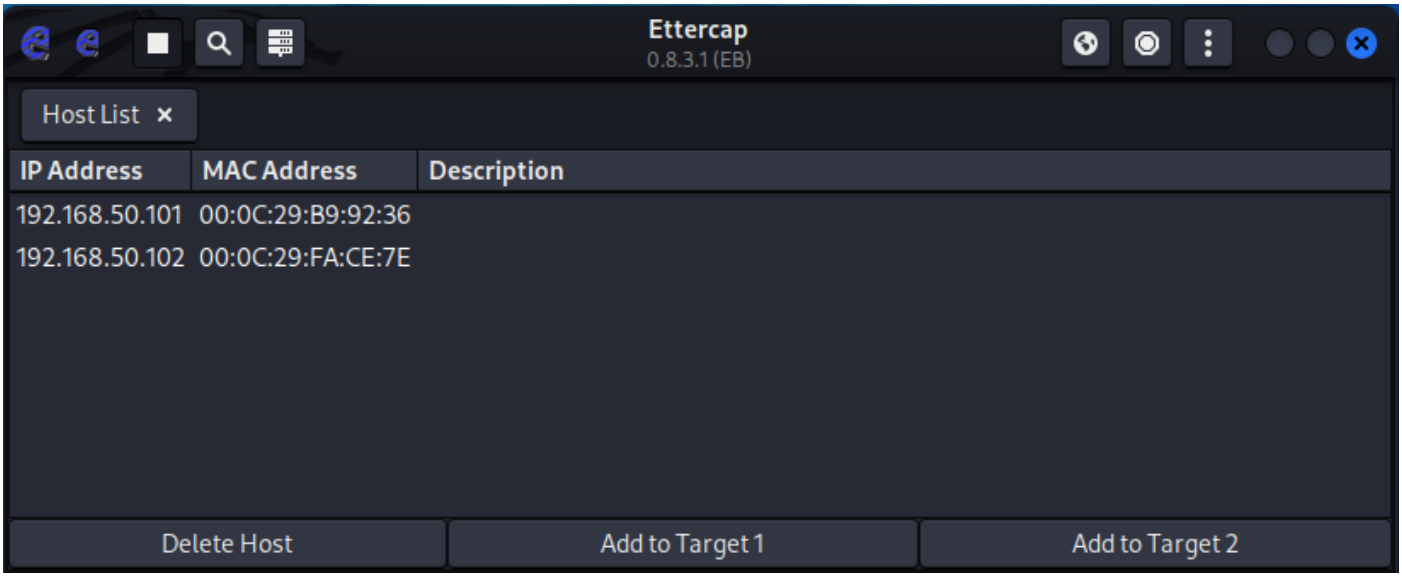


Dal menu, clicchiamo nella sezione *Host*s – *Scan fot hosts*



Una volta finito lo scan, entriamo nella sezione *Host list,* dove troviamo la lista degli host trovati,

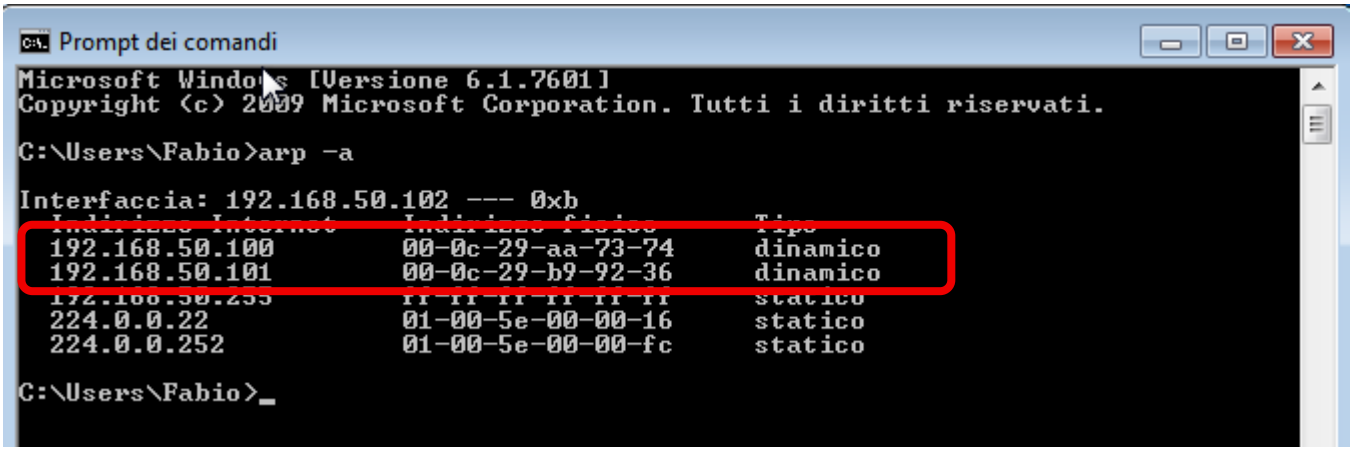
Selezioniamo quindi una alla volta i due host da attaccare, e aggiungiamoli come target, cliccando su *Add to targer 1/2*



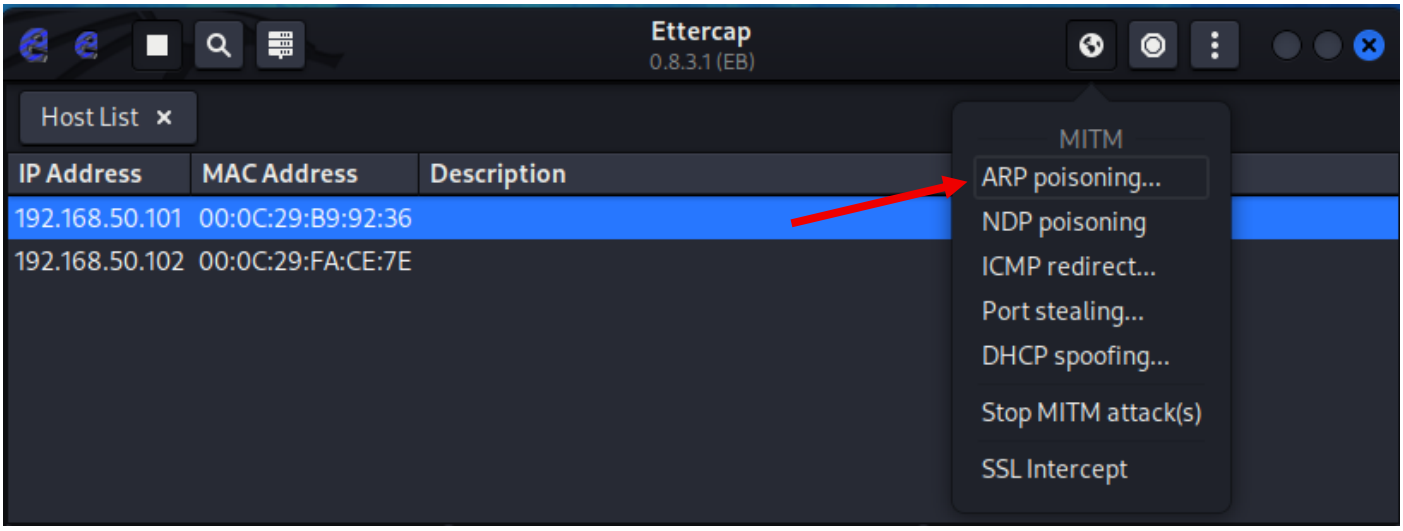
Prima di avviare l'attacco, possiamo visualizzare, dal prompt dei comandi di Windows 7, la tabella ARP degli Host collegati, tramite il comando `arp -a`, dove notiamo gli indirizzi MAC dei sistemi Kali e Metasploitable.

- 192.168.50.100 KALI

- 192.168.51.101 Metasplotable

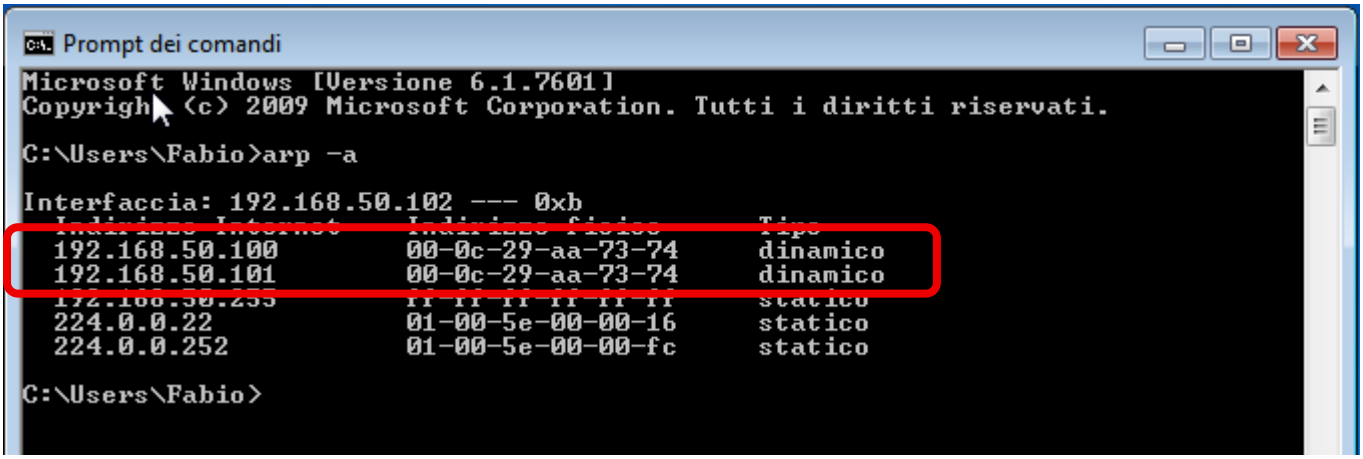


Avviamo ora l'attacco, tramite il tasto del "mondo" in alto, e successivamente *ARP Poisoning*



Una volta avviato l'attacco, possiamo ricontrollare la tabella ARP da Windows.

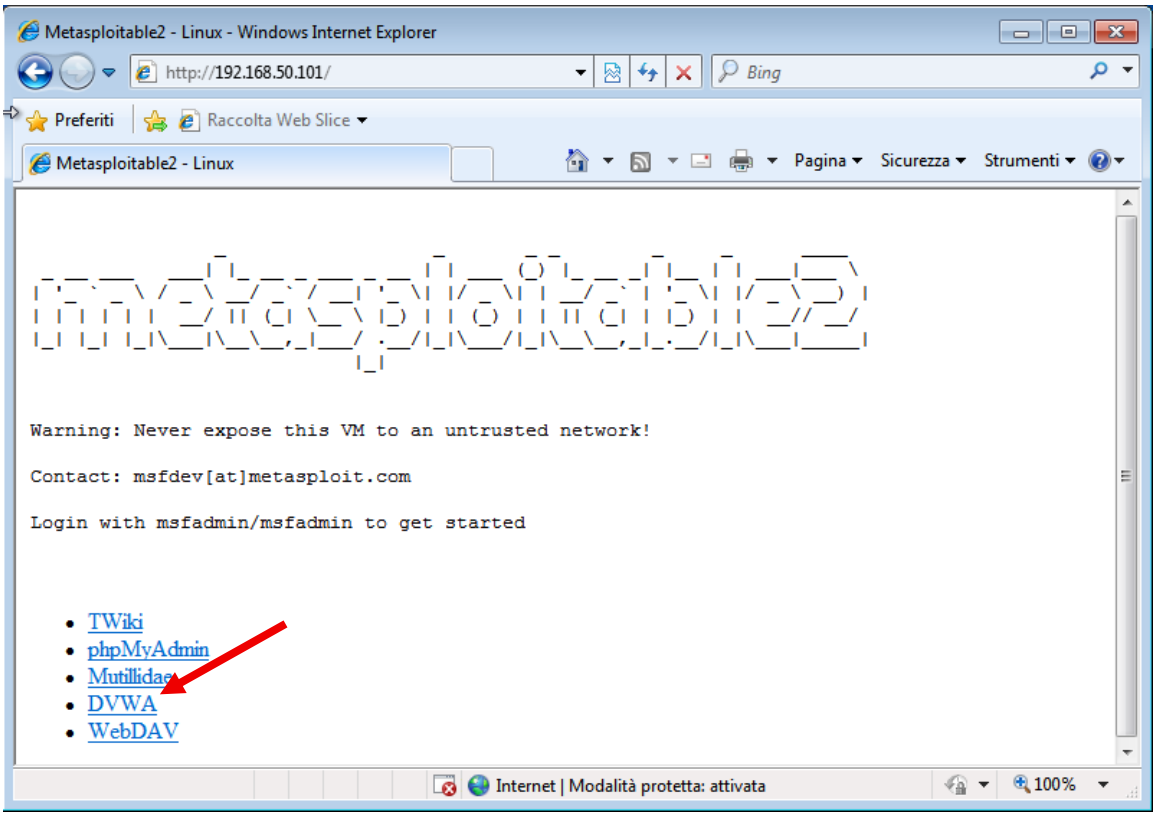
Possiamo notare come l'indirizzo MAC di Metasploitable sia cambiato, diventando uguale a quello di KALI, che quindi potrà intercettare le comunicazioni che non dovrebbero essere destinate a lui.



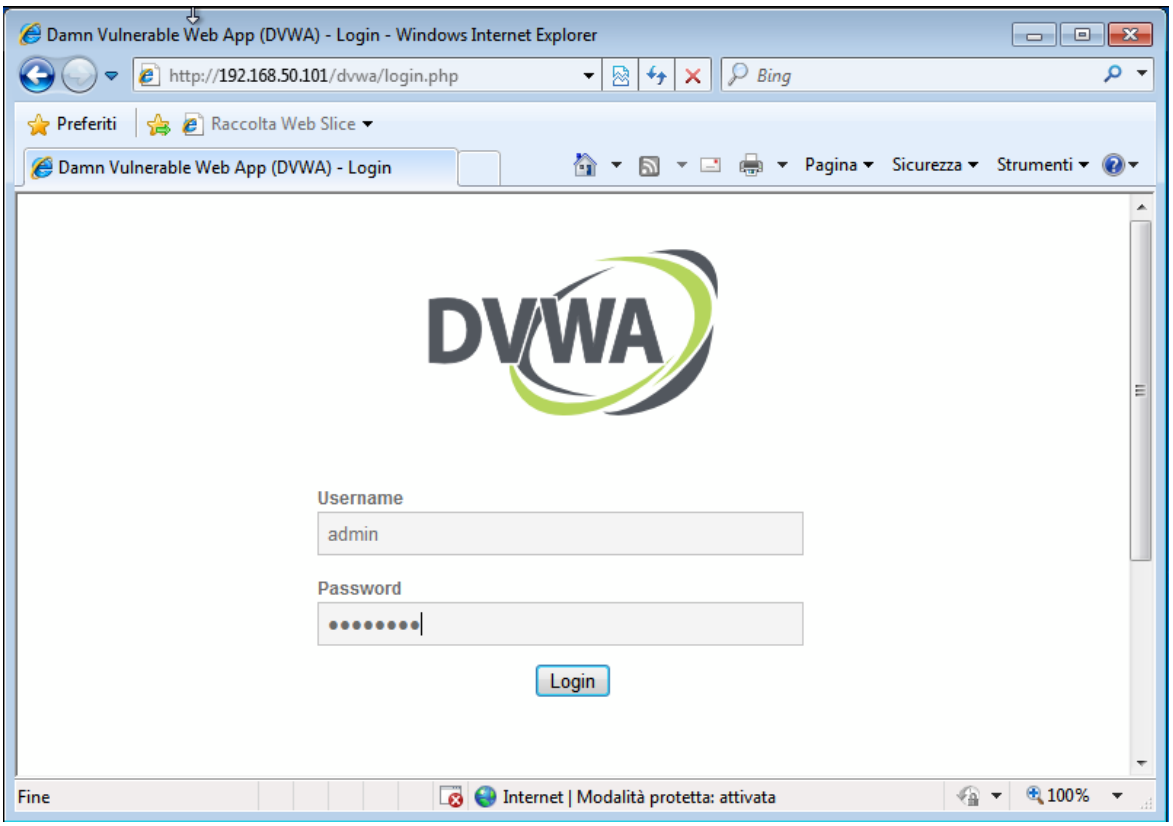
Per verficare l'effettivo funzionamento del ARP poisoning, avviamo uno scambio di dati tra i due sistemi attaccati.

Innazitutto, da Kali, avviamo Wireshark in ascolto per intercettare i pacchetti, e lo lasciamo in background.

Quindi, dal Browser di Windows colleghiamoci al servizio HTTP di Metsploitable.

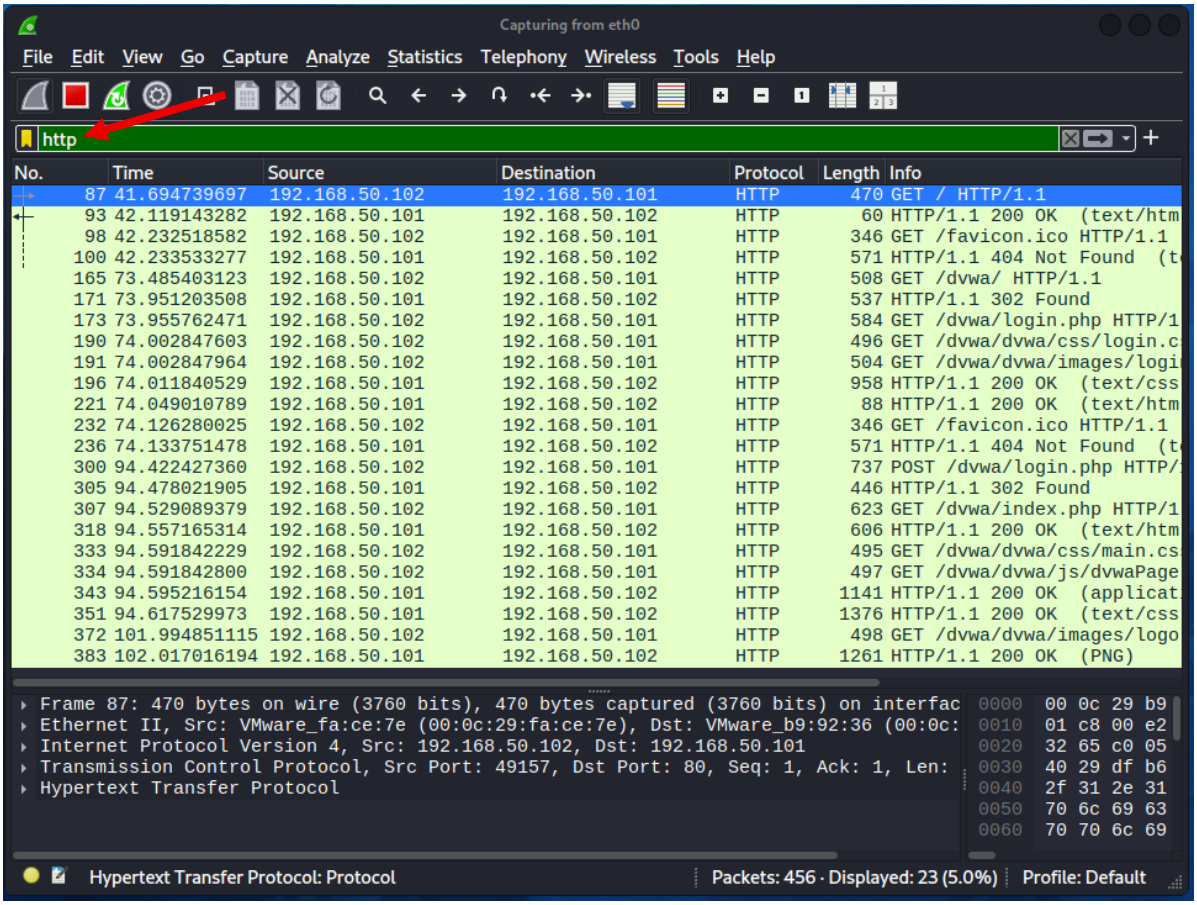


Entriamo nella pagina della DVWA ed inseriamo le credenziali di accesso (admin -password)



Ora torniamo su Kali e controlliamo i pacchetti intercettati da WireShark.

Il nostro scopo è intercettare le credenziali inserite in precedenza, quindi applichiamo un filtro “http” per visualizzare solo i pacchetti di questo protocollo.



Le credenziali, solitamenre, vengono inserite tramite le richieste POST, analizziamo quindi l’unica richiesta POST della lista.

Tra i dati della richiesta compaiono le credenziali inserite da Windows e destinate a Metsploitable.

L’ attacco è andato a buon fine