

W15D1 – NULL SESSION (anonymous logon)

Le *null session* sono vulnerabilità dello share di Windows (cartelle, file) e che sono ancora presenti in numerosi contesti aziendali. Tramite gli attacchi *null session* si possono recuperare informazioni dal target come ad esempio: password, programmi aperti, nomi utente di sistema ecc... perchè il sistema non richiede credenziali di autenticazione. Sfruttando questa vulnerabilità l'attaccante può connettersi da remoto utilizzando una condivisione amministrativa locale o remota.

Possiamo ancora trovare sistemi vulnerabili a questo attacco che sono:

windows explorer.exe;

windows xp 2003;

Samba linux/unix;

Le azioni di rimedio per questo tipo di vulnerabilità possono essere la rimozione del protocollo SMBV1 ovvero un protocollo obsoleto che permetteva ad un client di scrivere e leggere file su un server e non supporta la crittografia dei dati oppure l'utilizzo di chiavi LSA per impedire l'enumerazione delle share e l'enumerazione degli account.

Sono ovviamente necessarie anche attività di aggiornamento dei sistemi oppure blocco definitivo di utilizzo di attrezzature ormai obsolete.

ARP POISONING

Attacco che consiste nella manipolazione della tabella Arp cache che traduce i Mac address in indirizzi IP. Tramite questo attacco si possono inviare pacchetti ARP manipolati cosicché il traffico destinato ad un indirizzo MAC venga fatto deviare sull'indirizzo dell'attaccante. In questo modo l'attaccante intercetta, modifica, legge, il traffico di rete tra due host. (man in the middle)

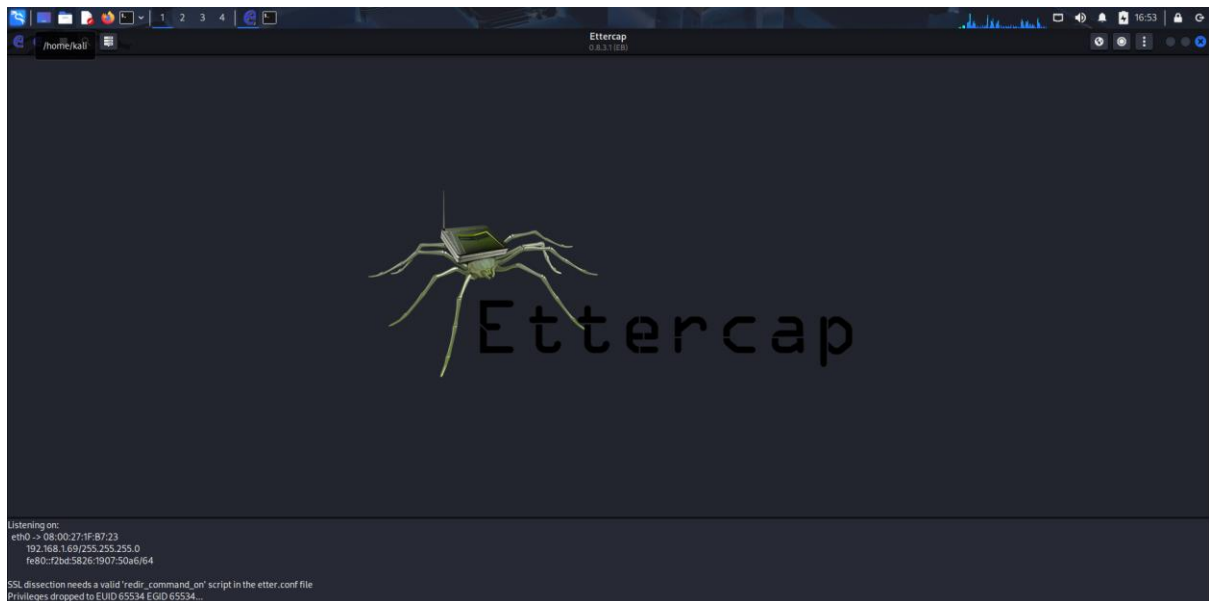
Le azioni di rimedio per evitare attacchi di questo comprendono: pulizia della cache, utilizzo di port security che imita il numero di indirizzi MAC che possono connettersi a una singola porta dello switch impedendo a un attaccante di inviare tante richieste; utilizzo di firewall per rilevare gli attacchi, utilizzo di protocollo https.

Esercizio con il tool ETTERCAP

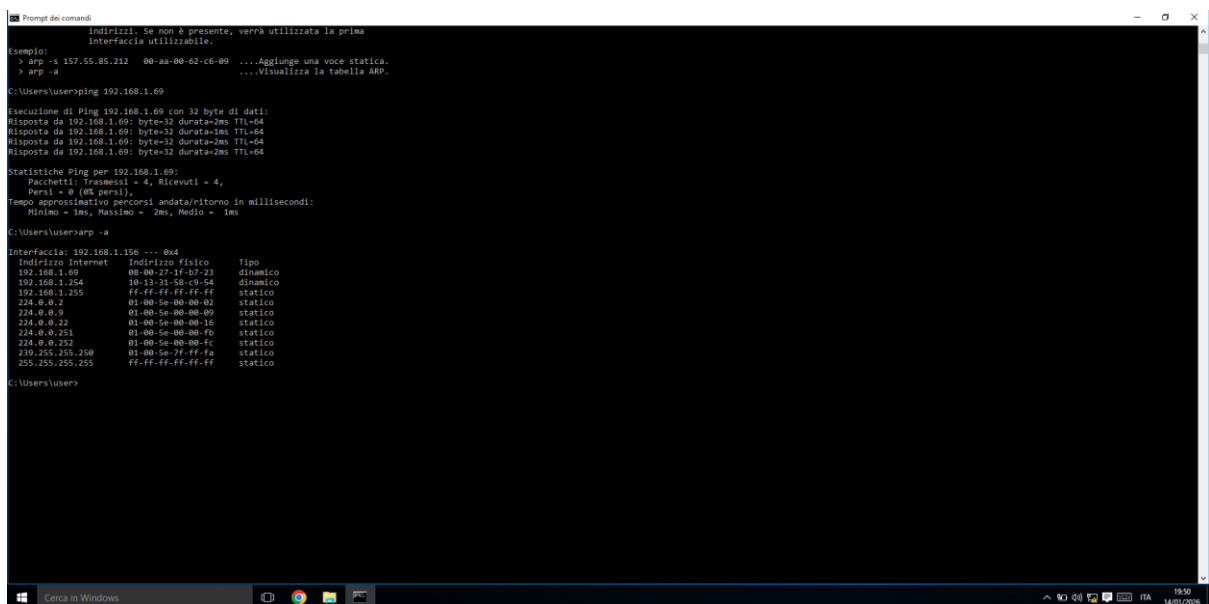
Si utilizza il tool ettercap come strumento di attacco di tipo Man in the middle per intercettare comunicazioni, analisi di rete o attacchi di spoofing.

Per l'esercizio facciamo partire una scansione degli hosts sulla nostra rete

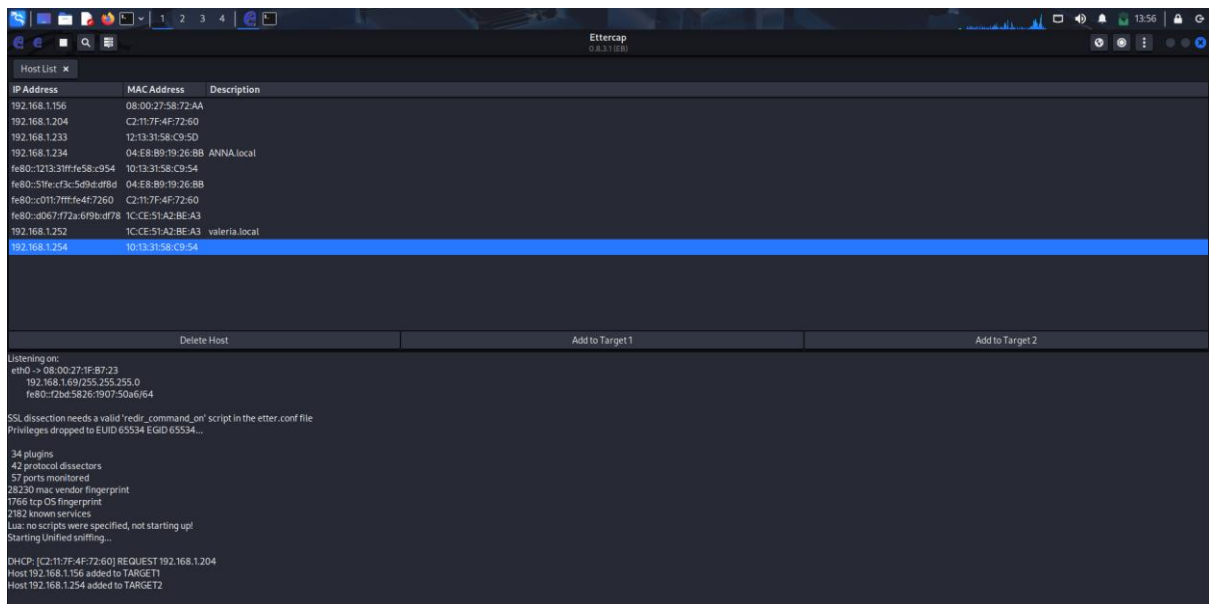
Indirizzo ip kali



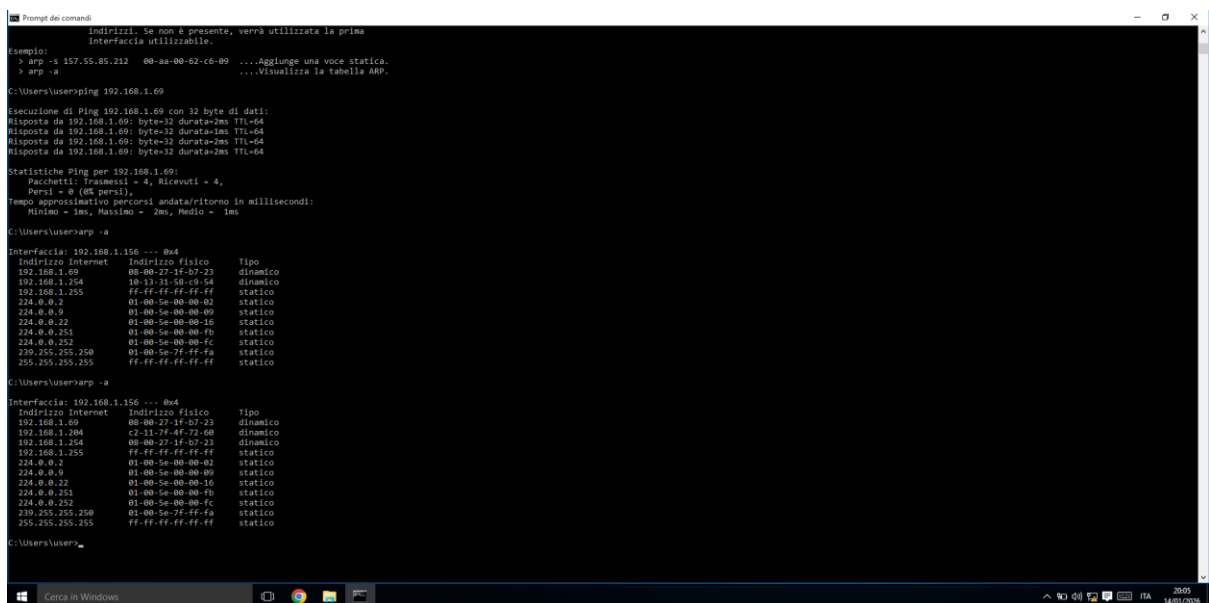
Risultato scansione



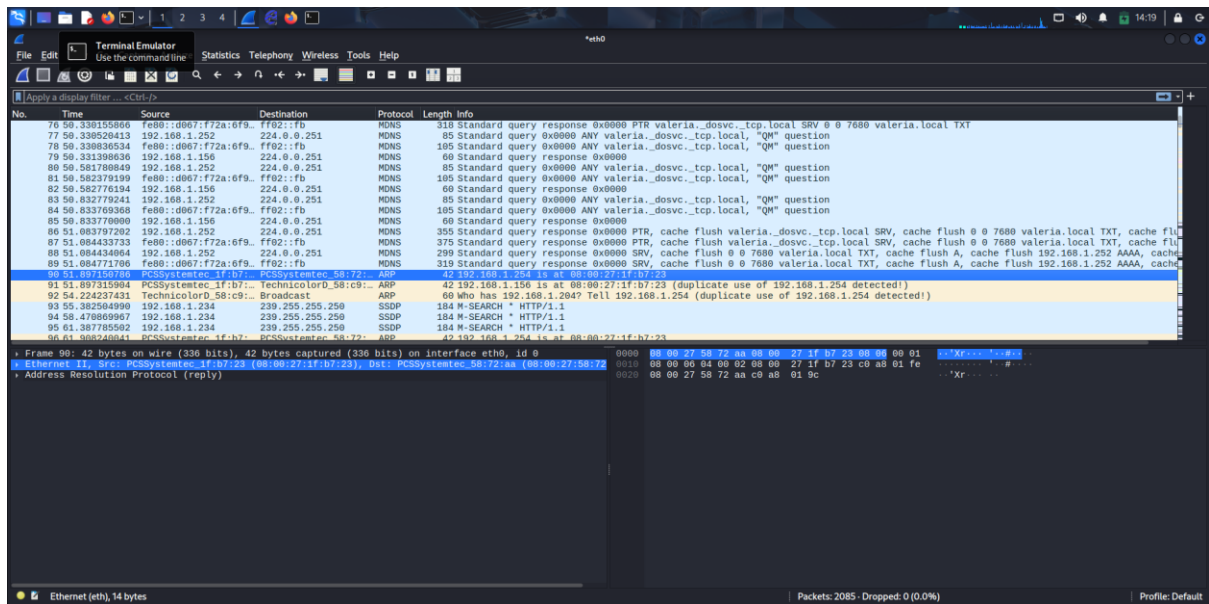
Troviamo l'ip della windows 192.168.1.156, il gateway 192.168.1.254 con mac address 10:13:31:58:C9:54 e l'ip 192.168.1.69 della kali con mac address 08:00:27:1f:b7:23



Adesso lanciamo l'attacco arp poisoning e vediamo che il mac address del gateway è cambiato ed è identico a quello della kali. L'attacco è riuscito in quanto lo scopo era proprio quello di intercettare la comunicazione andando a modificare i mac address che permettono all'attaccante di interpersi tra due host e sniffare le comunicazioni.

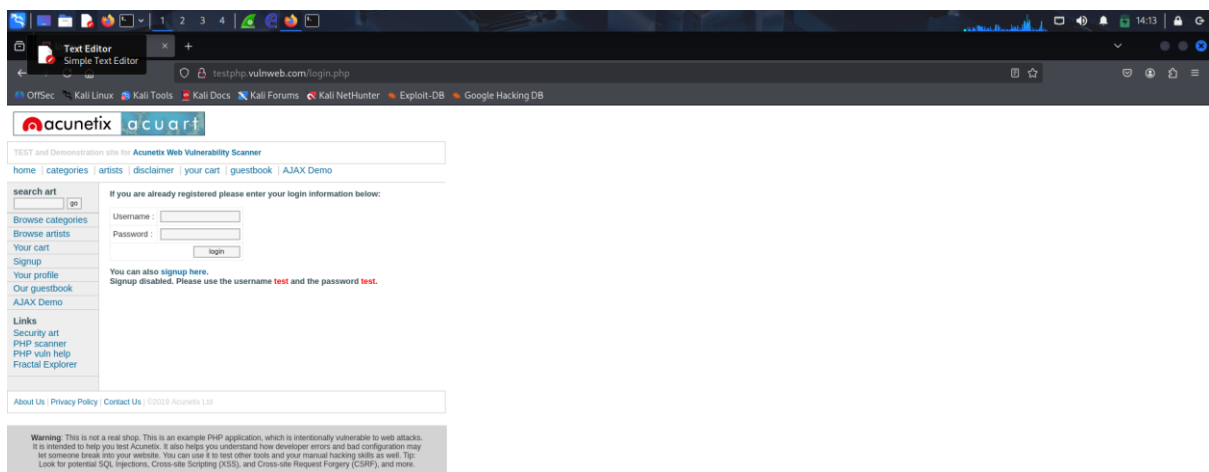


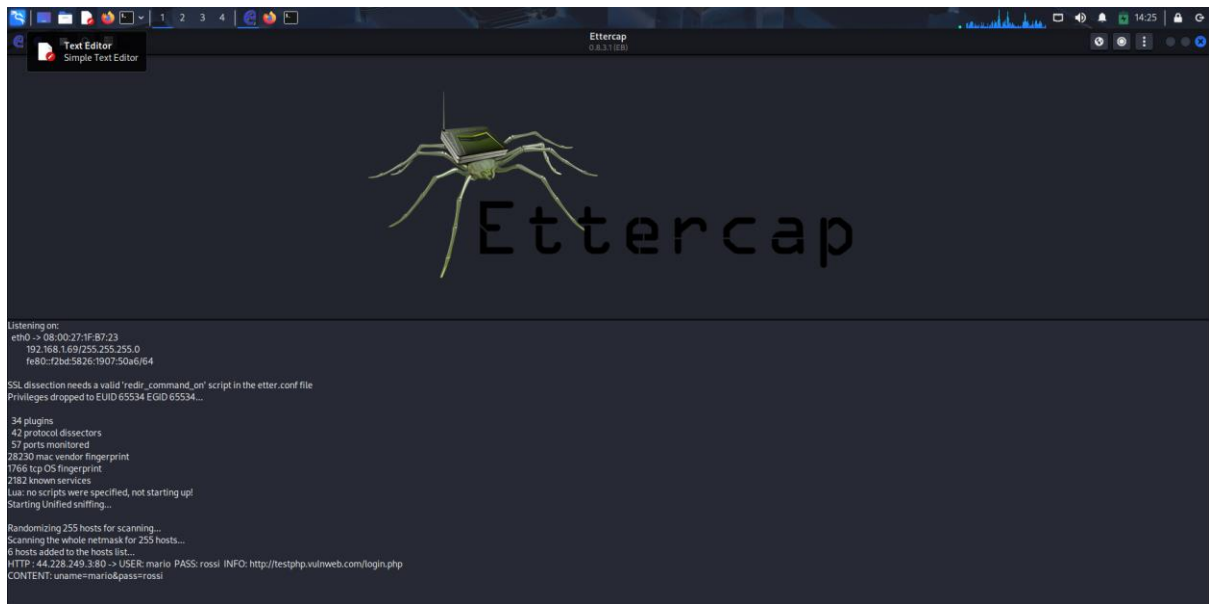
Si ha la controprova con wireshark e dunque si lancia una cattura per osservare i pacchetti trovati



si vede come il gateway ha preso il mac address della kali.

Ora si cerca di andare su una pagina web vulnerabile per tentare un altro attacco





Vediamo come siamo riusciti ad intercettare una comunicazione ed ad ottenere username e password per entrare in una pagina web privata.