"**Null session**" si riferisce a una vulnerabilità o a un exploit che coinvolge una sessione di connessione senza autenticazione su un sistema operativo di rete. Quando un client si connette a un server, può avviare una sessione senza fornire le credenziali di accesso, inserendo come credenziali ' ', campo che il Sistema Operativo interpreta come "sempre vero" e sfruttando questa vulnerabilità. In passato, i sistemi operativi Windows NT e le loro varianti come Windows 2000 e Windows XP erano noti per essere vulnerabili a questa falla di sicurezza. Di fatto le versioni citate dovrebbero essere "estinte". Microsoft ha comunque apportato modifiche significative alla sicurezza nel corso degli anni, quindi versioni più recenti come Windows 7, Windows 8 e Windows 10 non sono più soggette a questa vulnerabilità.Per mitigare o risolvere completamente la vulnerabilità della "null session", si elencano alcune metodologie che possono sembrare banali, ma sono sicuramente da considerare

- **Aggiornamento del sistema operativo**: Assicurati di avere la versione più recente del sistema operativo installato, poiché le nuove versioni solitamente correggono le vulnerabilità note.
- **Configurazione del firewall**: Impostaee un firewall per bloccare le connessioni non autorizzate e limitare l'accesso alle porte di rete necessarie.
- **Disabilitazione del supporto alla "null session"**: Alcuni sistemi operativi consentono di disabilitare completamente la possibilità di connessioni "null session". Verifica la documentazione del sistema operativo per ottenere istruzioni specifiche.
- **Accesso basato su account**: Configura il sistema operativo in modo che richieda sempre le credenziali di accesso per stabilire una connessione.
- **Politiche di sicurezza**: Implementa politiche di sicurezza aziendale che richiedono password robuste, limitano l'accesso privilegiato e promuovono le migliori pratiche di sicurezza informatica.

"**ARP Poisoning**" (o "**ARP Spoofing**") è una tecnica di attacco in cui un aggressore invia pacchetti ARP (Address Resolution Protocol) falsificati nella rete locale al fine di dirottare il traffico di rete, che deve necessariamente essere connessa da uno switch di qualsiasi tipologia. L'ARP viene utilizzato per mappare gli indirizzi IP degli host su indirizzi MAC nel livello di collegamento dei dati. In un attacco di ARP Poisoning, l'aggressore invia pacchetti ARP manipolati in cui asserisce di possedere un indirizzo MAC legato a un determinato indirizzo IP. Questo porta gli altri dispositivi nella rete a inviare il traffico verso l'aggressore anziché al dispositivo legittimo associato all'indirizzo IP. In questo modo, l'aggressore può intercettare o modificare il traffico di rete tra i dispositivi. I sistemi operativi che utilizzano il protocollo ARP, come Windows, Linux, macOS e molti dispositivi di rete, possono essere vulnerabili all'ARP Poisoning. Tuttavia, è importante notare che questa non è una vulnerabilità specifica di un sistema operativo, ma una debolezza nel funzionamento del protocollo ARP stesso. Per mitigare o risolvere l'ARP Poisoning, ecco alcune misure che possono essere adottate:

- **Monitoraggio della rete**: Utilizza strumenti di monitoraggio della rete per individuare anomalie nel traffico ARP e identificare eventuali attacchi di ARP Poisoning in corso.
- **Configurazione delle tabelle ARP**: Configura manualmente le tabelle ARP sui dispositivi di rete per associare gli indirizzi IP agli indirizzi MAC dei dispositivi legittimi. In questo modo, si riduce la possibilità di dirottamento del traffico.
- **Uso di tecnologie di sicurezza avanzate**: Alcuni dispositivi di rete o software di sicurezza possono offrire funzionalità di rilevamento e prevenzione dell'ARP Poisoning. Considera l'implementazione di tali soluzioni per migliorare la sicurezza della rete.
- **Uso di VLAN: Le VLAN** (Virtual Local Area Networks) possono separare il traffico di rete in segmenti logici, riducendo così la superficie di attacco per l'ARP Poisoning.
- **Crittografia del traffico**: L'utilizzo di protocolli di crittografia come HTTPS o VPN per proteggere il traffico di rete da eventuali manipolazioni o intercettazioni.