W15D1 - Pratica

Null Session

Che cos'è una Null Session?

Una Null Session è una particolare vulnerabilità dei servizi di Windows. Attraverso questa vulnerabilità è possibile da remoto accedere ad una serie di informazioni di un sistema quali password, gruppi, servizi, utenti e persino processi attivi. L'accesso alla sessione Null può essere utilizzato per eseguire attacchi DoS

Sistemi vulnerabili a Null Session

I sistemi operativi Windows che storicamente sono stati vulnerabili a Null Session includono:

- **Windows NT 4.0**
- **Windows 2000**
- **Windows XP**
- **Windows 2003**

Questi sistemi non sono più mantenuti e aggiornati da Microsoft. Tuttavia, potrebbero ancora essere presenti in alcuni sistemi legacy o ambienti che non sono stati aggiornati.
Dopo Windows 2003, Microsoft ha iniziato a introdurre restrizioni che riducono drasticamente l'uso delle Null session.

Mitigazione e risoluzione della Null session

- **Aggiornamento del sistema operativo**: Aggiornare a versioni moderne di Windows che includono patch di sicurezza contro Null Session.

- **Configurazione delle policy di sicurezza**: Modificare le impostazioni di sicurezza per limitare o disabilitare completamente l'accesso anonimo alle risorse di rete. Questo può essere fatto attraverso la Group Policy o tramite il registro di sistema.
- **Firewall**: Configurare firewall per bloccare l'accesso non autorizzato alle porte utilizzate da SMB (tipicamente porta 445).
- **Disabilitare l'accesso anonimo**: Nei sistemi che ancora permettono l'accesso anonimo, è possibile disabilitarlo tramite le impostazioni del registro di sistema o delle policy di sicurezza.

ARP Poisoning

Che cos'è l'ARP Poisoning?

L'ARP (Address Resolution Protocol) Poisoning, anche noto come ARP Spoofing, è un tipo di attacco di rete in cui un attaccante invia messaggi ARP falsificati su una rete locale. Questi messaggi ingannano i dispositivi nella rete facendoli credere che l'indirizzo MAC dell'attaccante corrisponda all'indirizzo IP di un altro dispositivo (spesso il gateway o un altro host). Questo permette all'attaccante di intercettare, modificare o interrompere il traffico di rete tra i dispositivi.

Sistemi vulnerabili a ARP Poisoning

Tutti i dispositivi collegati a una rete Ethernet che utilizzano ARP per la risoluzione degli indirizzi IP sono vulnerabili a ARP Poisoning. Questo include:

- **Router e Switches**: Anche se dispositivi di rete avanzati possono avere protezioni, sono comunque potenzialmente vulnerabili.
- **PC e Server**: Qualsiasi computer collegato a una rete LAN può essere un target.
- **Dispositivi IoT**: Molti dispositivi IoT non hanno protezioni contro questo tipo di attacco.

In pratica, qualsiasi rete locale Ethernet che non utilizza misure di sicurezza specifiche può essere vulnerabile.

Mitigazione, rilevazione e annullamento dell'attacco

- **Criptazione del traffico di rete**: Implementare protocolli di criptazione (es. IPsec, HTTPS) per assicurare che anche se un attacco ARP Poisoning ha successo, l'attaccante non può facilmente leggere o manipolare i dati intercettati.
- **Segmentazione della rete**: Utilizzare VLAN e altre tecniche di segmentazione della rete può limitare l'impatto di un attacco ARP Poisoning.
- **Implementare Dynamic ARP Inspection (DAI)**: Su switch gestiti, DAI può essere configurato per bloccare pacchetti ARP non validi.