Raul Pastor

Null Session e ARP Poisoning

Nell'esercizio di oggi viene richiesto di rispondere alle seguenti domande (anche attraverso delle ricerche su internet):

- 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.

1) Una Null Session è una connessione a un servizio di rete (solitamente tramite il protocollo SMB) che avviene senza fornire un nome utente o una password

2) Elenco dei sistemi operativi vulnerabili:

   - Windows NT 4.0 / Windows 95 / Windows 98: Vulnerabilità totale e nativa.
   - Windows 2000 / Windows XP (versioni iniziali): Permettevano l'accesso anonimo alla pipe IPC$ per elencare account e condivisioni.
   - Windows Server 2003: Ancora vulnerabile se non patchato o configurato con restrizioni specifiche (RestrictAnonymous).
   - Vecchie versioni di Samba (pre-3.0): Spesso implementate su vecchi NAS o sistemi Linux datati, esponevano le stesse informazioni dei sistemi Windows coevi.

3) Utilizziamo Enum4linux per la fase di verifica. Se si vedono liste di utenti o SID senza aver inserito una password, la Null Session è attiva (es: enum4linux -n <IP_TARGET>)

   WINDOWS:

   Per la fase di mitigazione nei sistemi moderni (Windows 10/11, Server 2019/2022), queste impostazioni sono solitamente sicure, ma vanno verificate.

   1. Editor del Registro di sistema: Vai al percorso: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
      - Trova il valore RestrictAnonymous.
      - Impostalo a 1 (impedisce l'enumerazione) o 2 (massima restrizione, potrebbe rompere la compatibilità con sistemi molto vecchi).
   2. Criteri di Gruppo (GPO): Se sei in un dominio Active Directory, il metodo corretto è tramite GPMC.msc:

  - Configurazione computer -> Impostazioni di Windows -> Impostazioni sicurezza -> Criteri locali -> Opzioni di sicurezza.
  - Abilita: "Accesso alla rete: limita l'accesso anonimo a Named Pipes e condivisioni".
  - Disabilita: "Accesso alla rete: consenti l'applicazione di autorizzazioni Anonymous a tutti gli utenti".

LINUX:

Se gestisci un server Linux che condivide file, devi agire sul file /etc/samba/smb.conf.

1. Apri il file: sudo nano /etc/samba/smb.conf
2. Nella sezione [global], verifica o aggiungi queste righe:

   ```
   [global]
   restrict anonymous = 2
   map to guest = Never
   ```

3. Assicurati che non ci siano condivisioni (share) con l'opzione guest ok = yes se non strettamente necessario.
4. Riavvia il servizio: sudo systemctl restart smbd

4) In un attacco ARP Poisoning, l'attaccante invia pacchetti ARP falsificati nella rete locale, in modo che il traffico destinato a un determinato indirizzo MAC venga deviato verso l'attaccante anziché verso il destinatario previsto. Ciò consente all'attaccante di intercettare e modificare il traffico di rete tra due host.

5) (SISTEMI OPERATIVI)
   Qualsiasi computer moderno è vulnerabile perché "si fida" delle risposte ARP che riceve. Se un attaccante invia un pacchetto ARP dicendo "Io sono il router", il computer della vittima aggiorna la sua ARP Cache senza verificare l'identità dell'attaccante.

   (DISPOSITIVI IoT e SMART HOME)
   Questa è la categoria più colpita oggi. Telecamere IP, lampadine smart, smart TV e sensori industriali spesso non hanno difese avanzate a livello di rete.

   (SWITCH E APPARATI DI RETE)
   Più che i singoli PC, la vulnerabilità dipende dagli Switch a cui sono collegati.

   Switch "Unmanaged" (Economici): Quelli che compri per casa o piccoli uffici non hanno protezioni. Inoltrano i pacchetti ARP malevoli senza controllo.

   Switch "Managed" (Professionali): Sistemi come Cisco, Juniper o Aruba hanno protezioni integrate (DAI - Dynamic ARP Inspection), ma spesso non vengono attivate dagli amministratori per pigrizia o mancanza di competenze.

Raul Pastor

6) Puoi vedere se sei sotto attacco controllando la tua tabella ARP locale. Se vedi due indirizzi IP diversi con lo stesso indirizzo MAC, sei vittima di spoofing:

```
# Su Windows o Linux
arp -a
```

Mitigazione:

1. DAI (Dynamic ARP Inspection): Sugli switch, incrocia i messaggi ARP con il database dei DHCP lease per bloccare i pacchetti falsi.
2. Port Security: Limita il numero di indirizzi MAC che possono collegarsi a una singola porta dello switch.
3. VPN e HTTPS: Non impediscono l'ARP Poisoning, ma rendono i dati catturati dall'attaccante illeggibili perché criptati.
4. Tabelle ARP statiche: Per server critici, si può mappare manualmente l'IP del gateway al suo MAC, impedendo al sistema di accettare aggiornamenti automatici.

Nel seguente screenshot ho incluso la prova di ARP Poisoning fatta in ambiente controllato inserendo delle credenziali su un sito con protocollo HTTP.