REPORT

Ho fatto la scansione delle vulnerabilità all' IP '192.168.50.20' che sarebbe la Metasploitable2 di VirtualBox. Ho scelto la Basic Network Scan, impostando il nome e l'IP; in DISCOVERY ho impostato 'Custom' e quindi in 'Port Scanning' ho spuntato 'Consider unscanned ports as closed' e ho inserito le porte: '21, 22, 23, 25, 80, 110, 139, 443, 445, 3389' in Port Scan Range. Ho scelto 'Verify open TCP ports found by local port enumerators' per avere risultati solo sulle porte scelte. Lasciando tutto il resto in default. Ho effettuato la scansione e ho creato i due Report in PDF in allegato.
Studiando le vulnerabilità trovate mi sono documentato su alcune di esse:

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Questa vulnerabilità riguarda una debolezza legata alle chiavi host SSH generate su sistemi Debian o Ubuntu che utilizzano una versione specifica della libreria OpenSSL con un bug nel generatore di numeri casuali. Ecco una spiegazione dettagliata:

Dettagli della vulnerabilità:

- Problema: Il problema è dovuto a una modifica nel pacchetto Debian di OpenSSL che ha ridotto drasticamente la quantità di "entropia" (casualità) utilizzata durante la generazione delle chiavi crittografiche. Questo rende le chiavi prevedibili.
- Effetto: Le chiavi SSH generate su queste versioni di Debian o Ubuntu sono deboli e possono essere facilmente compromesse.
- Rischio:
- Un attaccante può ottenere la parte privata della chiave SSH host.
- Questo gli consente di decifrare il traffico, effettuare attacchi "man-in-the-middle" o prendere il controllo remoto del server.

Soluzione:

1. Rigenerare le chiavi SSH:
   - È necessario rigenerare tutte le chiavi SSH che sono state create utilizzando le versioni vulnerabili della libreria OpenSSL.
   - Utilizzare un generatore di numeri casuali sicuro per assicurare una buona entropia.
2. Aggiornare OpenSSL:
   - Installare una versione aggiornata e sicura della libreria OpenSSL.
3. Verifica delle chiavi:
   - Strumenti come ssh-vulnkey possono essere utilizzati per verificare se una chiave SSH è affetta dal problema.

Questa vulnerabilità è nota come parte del problema storico della debolezza crittografica di Debian nel 2008, che ha influenzato molti sistemi.

32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Questa vulnerabilità è strettamente correlata alla precedente, ma riguarda nello specifico le chiavi SSL (certificate x509) generate su sistemi Debian o Ubuntu vulnerabili. Ecco la spiegazione:

Dettagli della vulnerabilità:

- Problema: Le chiavi SSL utilizzano un generatore di numeri casuali compromesso (a causa di un bug introdotto nella libreria OpenSSL sui sistemi Debian/Ubuntu), che produce chiavi crittografiche deboli e prevedibili.
- Effetto:
- I certificati SSL x509 generati su sistemi affetti sono considerati insicuri.
- Un attaccante può calcolare la chiave privata corrispondente al certificato pubblico.
- Questo permette all'attaccante di:
- Decifrare le connessioni cifrate SSL/TLS.
- Effettuare attacchi "man-in-the-middle" per intercettare dati sensibili come password o altre informazioni private.

Implicazioni:

Questa vulnerabilità colpisce non solo i certificati SSL, ma anche altri materiali crittografici come le chiavi OpenVPN generate su macchine vulnerabili.

Soluzione:

1. Identificare i sistemi vulnerabili: Verificare se il server Debian o Ubuntu ha utilizzato una versione vulnerabile della libreria OpenSSL.
2. Rigenerare le chiavi crittografiche:
   - Tutti i certificati SSL generati sul sistema affetto devono essere invalidati e rigenerati su un sistema sicuro con una versione aggiornata di OpenSSL.
   - Ciò include anche eventuali chiavi utilizzate per VPN (ad esempio, OpenVPN).
3. Aggiornare la libreria OpenSSL:
   - Installare una versione aggiornata della libreria OpenSSL non affetta dal bug.
4. Rivalutare la sicurezza:
   - Tutti i sistemi che hanno utilizzato certificati compromessi devono essere rivalutati per verificare l'assenza di accessi non autorizzati.

Questa vulnerabilità rappresenta un rischio elevato per la riservatezza e l'integrità dei dati scambiati tramite connessioni SSL/TLS, rendendo necessaria una risposta immediata.

20007 - SSL Version 2 and 3 Protocol Detection

Questa vulnerabilità riguarda l'utilizzo dei protocolli SSL 2.0 e SSL 3.0, che sono ormai considerati insicuri a causa di numerosi difetti crittografici. Ecco la spiegazione:

Dettagli della vulnerabilità:

1. Protocolli insicuri:
   - SSL 2.0 e SSL 3.0 sono protocolli obsoleti che presentano numerose debolezze crittografiche.
   - Anche se non sono più ampiamente utilizzati, alcuni server potrebbero ancora accettare connessioni che li utilizzano, esponendosi a potenziali attacchi.
2. Problemi principali:
   - Schemi di padding insicuri con cifrari CBC: Questo difetto può essere sfruttato per attacchi di tipo "padding oracle" (ad esempio, POODLE).
   - Schemi di negoziazione e ripresa della sessione insicuri: Questi difetti possono consentire attacchi man-in-the-middle (MITM) o decifrazione delle comunicazioni.
3. Rischio:
   - Gli attaccanti possono sfruttare queste debolezze per intercettare o alterare le comunicazioni tra il server e il client.
   - Possono anche decrittare dati sensibili che dovrebbero essere protetti.

Raccomandazioni:

1. Disabilitare SSL 2.0 e SSL 3.0:
   - Configurare il server per accettare solo protocolli più moderni e sicuri, come TLS 1.2 o TLS 1.3.
   - Verificare che tutte le configurazioni dei client supportino questi protocolli sicuri.
2. Aggiornare le configurazioni:
   - Assicurarsi che il server utilizzi cifrari sicuri e moderni.
   - Verificare le impostazioni relative alla negoziazione della sessione.
3. Conformità agli standard:
   - SSL 3.0 non soddisfa più i requisiti di sicurezza definiti, ad esempio, dal PCI DSS (Data Security Standard). I sistemi che richiedono la conformità devono disabilitare qualsiasi versione di SSL.

Conclusione:

SSL 2.0 e SSL 3.0 sono protocolli insicuri che devono essere completamente disabilitati. Passare ai protocolli TLS più recenti è essenziale per garantire la sicurezza delle comunicazioni.