Report su alcune vulnerabilitá della Metasploitable nel dettaglio.  
SWEET32

Partiamo da una delle meno gravi.

La vulnerabilità SWEET32 riguarda un problema di sicurezza con certi tipi di cifrari utilizzati nei protocolli di sicurezza, come SSL/TLS, che proteggono le comunicazioni su Internet (per esempio, quando navighi su siti "https"). Alcuni di questi cifrari, come **3DES**, lavorano su "blocchi" di dati piuttosto piccoli, da 64 bit.

**Il problema**

Quando un cifrario usa blocchi piccoli, come quelli da 64 bit, può succedere che, dopo un certo numero di dati trasmessi, i blocchi iniziano a ripetersi (è un po' come avere troppe persone e pochi vestiti: prima o poi due persone avranno lo stesso vestito!). Queste ripetizioni permettono a un attaccante che osserva il traffico di cominciare a "intuire" cosa c'è dentro i dati cifrati. Con abbastanza informazioni, potrebbe riuscire a decrittarli o addirittura manipolarli.

Questo è il cuore del problema di SWEET32: se un attaccante riesce a vedere abbastanza dati cifrati (ad esempio, guardando il traffico di rete tra te e un server), potrebbe usarli per rompere la cifratura e vedere i dati sensibili, come password o informazioni personali.

**Come può succedere?**

SWEET32 non è una vulnerabilità facile da sfruttare. L'attaccante deve:

1. Osservare una connessione cifrata per un **tempo lungo** e catturare **molti dati cifrati**.
2. Approfittare del fatto che il server e il client usano un cifrario debole (come 3DES).

Ma con tempo e risorse sufficienti, può essere fatto.

**Perché succede con 3DES e cifrari simili?**

Il problema non è tanto il tipo di cifratura, ma la **dimensione dei blocchi**. Cifrari come 3DES usano blocchi di soli 64 bit, che ormai sono considerati troppo piccoli per garantire una buona sicurezza. I cifrari più moderni, come AES, usano blocchi da 128 o 256 bit, che rendono quasi impossibile trovare ripetizioni di blocchi anche con enormi quantità di dati.

**Come risolvere il problema?**

La soluzione è semplice: basta **evitare di usare cifrari deboli come 3DES**. Ecco come si fa:

1. **Aggiornare il server**: configurare il server web per usare cifrari moderni come AES (Advanced Encryption Standard) e protocolli più recenti, come TLS 1.2 o 1.3.
2. **Verificare la sicurezza**: strumenti come **Qualys SSL Labs** possono controllare la configurazione di un server e dire se ci sono cifrari vulnerabili ancora attivi.

**UnrealIRCd Backdoor Detection**

Immagine che contiene testo, schermata, software

Descrizione generata automaticamente

La vulnerabilità **UnrealIRCd Backdoor Detection** riguarda una versione compromessa del software **UnrealIRCd**, che è un popolare server per chat IRC (Internet Relay Chat).

In pratica, qualcuno aveva distribuito una versione modificata di UnrealIRCd con una "backdoor" nascosta. Una **backdoor** è un accesso segreto che permette a un attaccante di entrare nel server senza autorizzazione. In questo caso specifico, un attaccante poteva eseguire comandi malevoli sul server semplicemente inviandogli un comando speciale.

**Perché è grave?**

Chiunque fosse a conoscenza della backdoor poteva:

* Prendere il controllo del server.
* Rubare o manipolare i dati.
* Usare il server per attacchi ad altri sistemi.

**Come si risolve?**

Per risolvere il problema è necessario:

1. **Eliminare la versione compromessa** e scaricare UnrealIRCd solo da fonti ufficiali.
2. **Aggiornare il software** all'ultima versione non compromessa.

In sintesi: è stata una trappola inserita in una versione "taroccata" del software, e la soluzione è assicurarsi di scaricare e usare solo versioni ufficiali e aggiornate.

Bind Shell Backdoor DetectionImmagine che contiene testo, schermata, software

Descrizione generata automaticamente

Una **bind shell backdoor** è una porta segreta che un attaccante apre su un computer per poterci entrare da remoto. Questa "porta" resta in ascolto, pronta ad accettare connessioni, così l'attaccante può eseguire comandi e controllare il sistema senza permesso.

**Perché è grave?**

Perché l'attaccante può fare quello che vuole sul computer: rubare dati, installare virus o distruggere file.

**Come risolvere?**

* Bloccare la porta aperta.
* Rimuovere il programma o il file sospetto.
* Aggiornare e proteggere il sistema per evitare che succeda di nuovo.