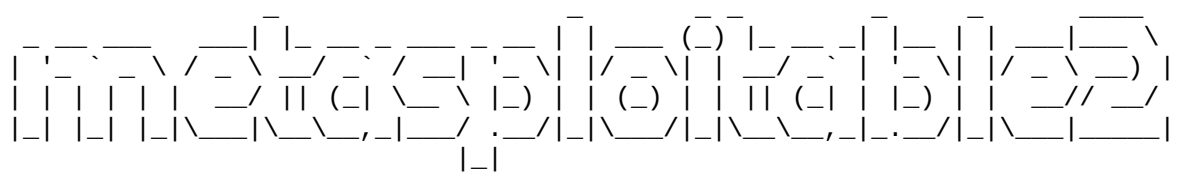

```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login:
------------------------------ snip ------------------------------
```

Medium: SSL Anonymous Cipher Suites Supported

Description

The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

Descrizione

L'host remoto supporta l'uso di crittografie SSL anonime. Sebbene ciò consenta a un amministratore di impostare un servizio che crittografa il traffico senza dover generare e configurare certificati SSL, non offre alcun modo per verificare l'identità dell'host remoto e rende il servizio vulnerabile a un attacco man-in-the-middle.

Nota: questo è molto più semplice da sfruttare se l'aggressore si trova sulla stessa rete fisica.

Solution

Reconfigure the affected application if possible to avoid use of weak ciphers.

Soluzione

```
Se possibile, riconfigurare l'applicazione interessata per evitare l'uso di
codici deboli.
```