CONSEGNA 6 MARZO S7L3

L'obiettivo di oggi è quello di ottenere una sessione di Meterpreter sul target Window xp sfruttando con Metasploit la vulnerbilità MS08-067. Una volta ottenuta la sessione, dovrò recuperare uno screenshot della interfaccia della vittima e individuare la presenza o meno di una Webcam.

Dopo aver impostato gli indirizzi IP delle macchine, ho avviato MSFConsole e ho cercato la vulnerabilità MS08-067. Con il comando search ho trovato l'exploit da usare, windows/smb/ms08_067_netapi, dove ho dovuto inserire l'indirizzo IP della vittima. Il payload consigliato era windows/meterpreter/reverse_tcp, quindi ho lanciato l'exploit e mi si e aperta una sessione di Meterpreter. Tramite questo potente strumento, sono riuscito a fare una screenshot dell'interfaccia della vittima e ho anche provato a vedere se la macchina target aveva una webcam. (Fig.1)

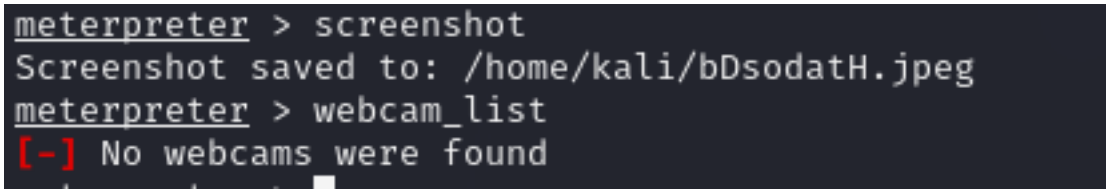

Fig.1

Come in figura, lo screenshot è stato salvato in /home/kali/bDsodatH.jpeg (Fig.2)

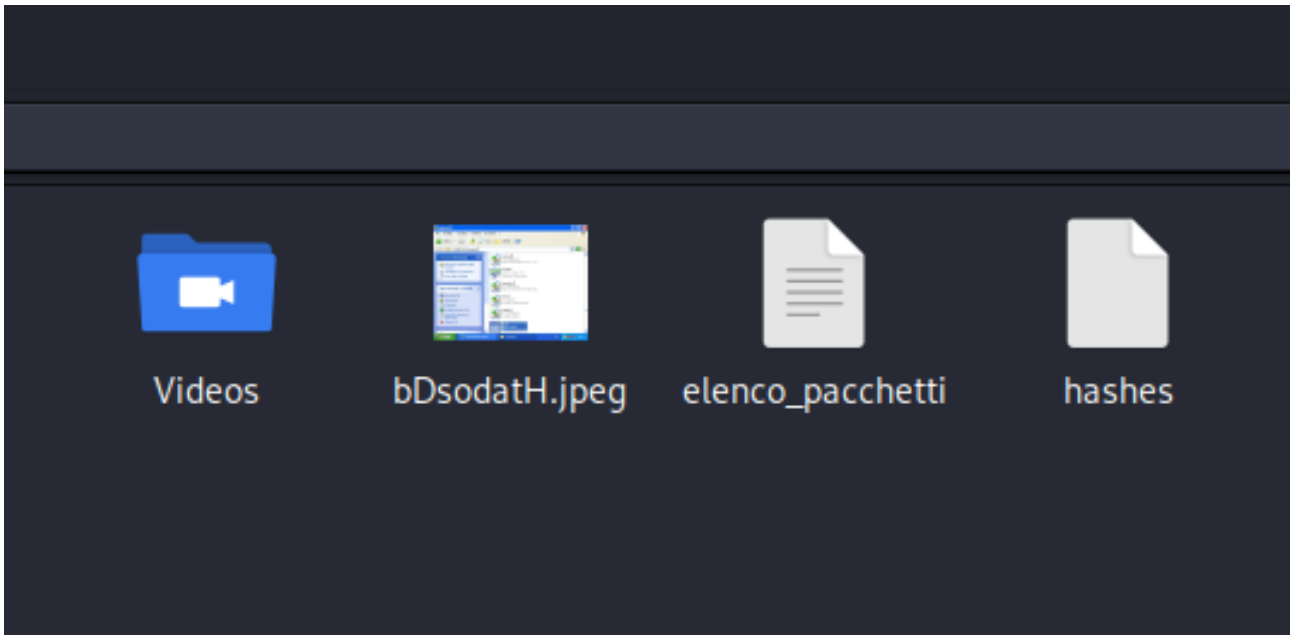

Fig.2

Per quanta riguarda la webcam, non ne sono state trovate.

Vorrei dilungarmi sulla vulnerabilità MS08-067.La vulnerabilità MS08-067 è stata una delle più significative e dannose vulnerabilità scoperte nei sistemi Windows. È stata identificata nel 2008 e colpiva specificamente il servizio Server di Windows. Questa vulnerabilità permetteva agli attaccanti di eseguire codice arbitrario sui sistemi vulnerabili senza autenticazione, rendendo i sistemi vulnerabili a un'ampia gamma di attacchi, inclusi quelli di tipo worm.
Un worm noto come Conficker, o Downadup, è stato uno dei più famosi malware a sfruttare questa vulnerabilità. Una volta infettato un sistema, Conficker poteva propagarsi automaticamente attraverso la rete, infettando altri sistemi Windows non ancora patchati con la correzione per la vulnerabilità MS08-067.

Microsoft ha rilasciato una patch per correggere questa vulnerabilità poco dopo la sua scoperta, ma molti sistemi non sono stati tempestivamente aggiornati, permettendo a Conficker e ad altri malware di sfruttare la vulnerabilità per diffondersi ampiamente.

La sigla <MF08-067> è stata assegnata da windows ed inserita nel Security Bulletin, che include una serie di aggiornamenti per risolvere le vulnerabilità scoperte.

- MS: indica Microsoft Security Bulletin.

- 08: l’anno di pubblicazione, quindi 2008 in questo caso.

- 067: numero progressivo del «Bulletin» pubblicato nel 2017, quindi in questo caso è il decimo.