Crackare il file SAM

Testo realizzato da FauleY

e-mail to: axel_fauley@yahoo.it
http://www.autistici.org/hackarena

Descrizione e vulnerabilità

Il file SAM, ovvero "Security Accounts Manager", contiene le credenziali di tutti gli utenti che hanno diritto all'autenticazione nel sistema.
Quando un utente invia la richiesta di autenticarsi al server tramite password, questo invia un "challenge" (sfida) al client dell'utente che risponderà con una "response" (risposta).
Il challenge è crittato secondo la password contenuta nel file SAM, e verrà confrontato con la chiave contenuta nell'hash inviato dal client (sarebbe a dire la password digitata dall'utente); se gli hash sono uguali, l'utente sarà autenticato all'interno del sistema server.
La vulnerabilità principale di questo sitema, data la debolezza del sitema di cifratura del file SAM, è la possibile decrittazione dell'algoritmo in tempi relativamente ristretti.
La sua collocazione in Windows NT è nella directory "%systemroot%\system32\conf" (senza apici), mentre negli altri sistemi Windows è locato nella directory "systemroot\system32\conf" (senza apici); il file non presenta estenzione.
Il file SAM non è direttamente prelevabile in quanto in uso dal sistema (dall'applicazione SYSKEY), quindi, dovremo utilizzare alcuni metodi che ci permetteranno di aggirare SYSKEY; abbiamo 4 differenti possibilità di prelevare il file SAM dal sistema:
Avendo accesso fisico al sistema server è possibile effettuare il boot con un altro sistema opeartivo in modo da non attivare SYSKEY e prelevare il file.
Prelevare una copia del file SAM dalla directory "%systemroot%\repair" (senza apici) in Windows NT e nella directory "system32\repair" (senza apici) in tutti gli altri sistemi Windows.
Estrarre gli hash del file con un programma creato da Todd Sabin ("pwdump3.exe").
Tramite la tecnica del MITM (ovvero "Man in the Middle"), sniffando le comunicazioni Server==>Client che avvengono secondo il protocollo "challenge/response".
==>Nel caso in cui la partizione del sistema sia di tipo NTFS un boot DOS nn sarà in grado di leggerle. Sarà indispensabile procurasi "NFTS DOS" (su "www.sysinternals.com") oppure utilizzare un sistema operativo di tipo *nix like.
==>Con privilegi di Administrator, nei sistemi Windows NT è possibile (nel caso in cui la directory sia vuota) ottenere una copia del file SAM nella directory "repair"eseguendo il comando dalla riga di comando "rdisk /s"
==> Il programma "pwdump3" utilizza un tipo di injection in una libreria dll per potere scrivere nella memoria di altri processi con autorizzazioni maggiori.
Questo tipo di attacco permette dunque a pwdump di inserire nello spazio di memoria del sistema "LSASS" (ovvero "Local Security Autority SubSystem") un codice eseguibile, ottenendo autorizzazioni maggiori che gli permettono di visualizzare gli hash del file SAM.
=>Il Man In the Middle (ovvero il MITM) applicato al file SAM consiste nello sniffaggio in una rete locale dei i pacchetti SMB contenenti gli hash con la chiave di autenticazione.
Per applicare questo tipo di attacco è possibile utilizzare il software del l0phtcrack, che tramite la funzione "SMB packet capture" ci fornisce gli hash di un utenete che sta effettuando un'autenticazione.
L'attaccante dovrebbe poi effettuare il brute-force per decrittarli e ottenere la password o inviare direttamente gli hash al server vittima mediante appositi programmi.

Crackaggio:

MISSING = password ASSENTE

BENCHMARK CRACKAGGIO
Lettere:

LUNGHEZZA	PERMUTAZIONI	AMD ATHLON @ 1GHz
01	26	< 1 secondo
02	676	< 1 secondo

03	17,576	< 1 secondo
04	456,976	< 1 secondo
05	11,881,376	04 secondi
06	308,915,776	02 minuti 19 secondi
07	8,031,810,176	01 ora 06 minuti 08 secondi
08	208,827,064,576	01 ora 06 minuti 05 secondi
09	5,429,503,678,976	01 ora 06 minuti 02 secondi
10	141,167,095,653,376	01 ora 06 minuti 05 secondi
11	3,670,344,486,987,776	01 ora 06 minuti 03 secondi
12	95,428,956,661,682,176	01 ora 06 minuti 05 secondi
13	2,481,152,873,203,736,576	01 ora 06 minuti 12 secondi
14	64,509,974,703,297,150,976	01 ora 10 minuti 14 secondi

Lettere e numeri:

LUNGHEZZA	PERMUTAZIONI	AMD ATHLON @ 1GHz
01	36	< 1 secondo
02	1,296	< 1 secondo
03	46,656	< 1 secondo
04	1,679,616	< 1 secondo
05	60,466,176	24 secondi
06	2,176,782,336	16 minuti 18 secondi
07	78,364,164,096	10 ore 41 minuti 57 secondi
08	2,821,109,907,456	10 ore 41 minuti 38 secondi
09	101,559,956,668,416	10 ore 41 minuti 48 secondi
10	3,656,158,440,062,976	10 ore 42 minuti 43 secondi
11	131,621,703,842,267,136	10 ore 41 minuti 48 secondi
12	4,738,381,338,321,616,896	10 ore 43 minuti 04 secondi
13	170,581,728,179,578,208,256	10 ore 44 minuti 33 secondi
14	6,140,942,214,464,815,497,216	11 ore 22 minuti 48 secondi

Lettere, numeri e caratteri speciali (uk)**

LUNGHEZZA	PERMUTAZIONI	AMD ATHLON @ 1 GHz
01	71	< 1 secondo
02	5,041	< 1 secondo
03	357,911	< 1 secondo
04	25,411,681	09 secondi
05	1,804,229,351	12 minuti 27 secondi
06	128,100,283,921	16 ore 20 minuti 47 secondi
07	9,095,120,158,391	circa 52 giorni, non testato completamente

** N.B. questo test e' stato effettuato con i caratteri speciali di una tastiera inglese, escluso l'euro, che sono
!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~£¬
C'e' da far notare che, pero', nella tastiera italiana il range si allarga notevolmente perche' si possono utilizzare anche le lettere accentate che, sulle tastiere straniere, sono digitabili solo grazie alla combinazione ALT + sequenza_numerica.