Session Start: Mon Nov 10 18:50:24 2003
Session Ident: #AlexMessoMalex
* Now talking in #AlexMessoMalex
* Topic is '•8,10•www.AlexMessoMalex.com•• •4,15Prossima parte del Chat-Meeting: lunedì 10 Nov ore 21.30• •0,2Si prega di visitare la sezione •8•FAQ••0 e il •8•FORUM••0 prima di chiedere ai moderatori.••'
* Set by SaNdStOrM on Thu Nov 06 20:48:51

<XSickBoyX> possiamo moderare e iniziare?
<SaNdStOrM> si
<XSickBoyX> ALLORA
<XSickBoyX> qualunque domanda
<XSickBoyX> che dovete fare
<XSickBoyX> le querate
<XSickBoyX> ad uno degli op
<XSickBoyX> e poi facciamo delle pause
<XSickBoyX> we rispondo ok????
<XSickBoyX> perfetto
<XSickBoyX> allora
<XSickBoyX> nelle ultime due lezioni
<XSickBoyX> ci siamo soffermati
<XSickBoyX> su
<XSickBoyX> i metodi x bekkare le hash delle password dal SAM di WinNT
<XSickBoyX> non le ripeto
<XSickBoyX> xkè altrimenti sprechiamo anche sta lezione
<XSickBoyX> cmq...
<XSickBoyX> volevo dire una cosa.....
<XSickBoyX> TUTTE QUESTE COSE CHE STO DICENDO VALGONO SU WIN NT
<XSickBoyX> WIN 2000 SARà IL PROSSIMO ARGOMENTO!!!!
<XSickBoyX> ok?
<XSickBoyX> andiamo avanti
<XSickBoyX> stasera parleremo delle crack delle hash delle pass
<XSickBoyX> e usiamo LophtCrack
<XSickBoyX> (dopo vedremo brevemente anche John The Ripper... lo so è antico come programma ma ancora efficace!)
<XSickBoyX> cmq
<XSickBoyX> parliamo di LophtCrack
<XSickBoyX> questa grande applicazione
<XSickBoyX> la troviamo su
<XSickBoyX> www.atstake.com/research/lc3/index.html
<XSickBoyX> e serve per fare tante belle cose
<XSickBoyX> il progr che scaricherete è trial
<XSickBoyX> ma si trova facilmente la key da inserire su astalavista.box.sk
* AlexMessoMalex sets mode: +m
<XSickBoyX> LC x crakkare le pass
<XSickBoyX> del SAM
<XSickBoyX> usa un attakko usando un dizionario di parole
<XSickBoyX> e se non riesce il primo usa un bruceforce
<XSickBoyX> e prima o poi la pass la bekkate
<XSickBoyX> è solo questione di tempo
<XSickBoyX> dopo ricordatemi di darvi il link
<XSickBoyX> x scaricare
<XSickBoyX> le liste di dizionari
<XSickBoyX> di parole in tutte le lingue
<XSickBoyX> xkè l'ho scritto
<XSickBoyX> ma nn lo trovo e nn voglio perdere tempo
<XSickBoyX> la versione
<XSickBoyX> di LC
<XSickBoyX> è la 4
<XSickBoyX> quindi parlo di quest'ultima
<XSickBoyX> cmq
<XSickBoyX> dopo ricordatemi il link
<XSickBoyX> allora
<XSickBoyX> LC è in grado
<XSickBoyX> di bekkarvi le pass
<XSickBoyX> sia da un file SAM preso con il metodo di reboot

<XSickBoyX> sia col file sam preso dalla directory repair
<XSickBoyX> inoltre
<XSickBoyX> LC permette
<XSickBoyX> di
<XSickBoyX> salvare
<XSickBoyX> il bruceforce
<XSickBoyX> in modo da tale da non ricominciare tutto d'accapo
<XSickBoyX> Inoltre
<XSickBoyX> LC ha
<XSickBoyX> una funzione
<XSickBoyX> x bekkare il sam
<XSickBoyX> SEMPLICEMENTE inserendo l'ip
<XSickBoyX> di un pc vittima
<XSickBoyX> xò questa tecnica nn funziona se il pc vittima
<XSickBoyX> ha la funzione SysKey attiva
<XSickBoyX> la maggior parte degli NT server praticamente
<XSickBoyX> :)
<XSickBoyX> ovviamente se c'è SysKey si usa pwdump2
<XSickBoyX> di cui abbiamo parlato
<XSickBoyX> la scorsa volta
<XSickBoyX> una volta ottenuto il sam
<XSickBoyX> utilizzando il menu file
<XSickBoyX> e l'opzione Session/Session Options
<XSickBoyX> potete impostare il tutto
<XSickBoyX> i dizionari da usare (x default c'è un dizionario inglese)
<XSickBoyX> le modalità di bruceforce ect
<XSickBoyX> PARDON
<XSickBoyX> Brute force
<XSickBoyX> dicevo...
<XSickBoyX> che
<XSickBoyX> altro attakko di LC
<XSickBoyX> è la funzione hybrid
<XSickBoyX> in che consiste?
<XSickBoyX> consiste nella possibilità di aggiungere fino a tre caratteri
<XSickBoyX> prima o dopo le parole di un dizionario
<XSickBoyX> tipo
<XSickBoyX> se la mia pass è giulio81
<XSickBoyX> e nel dizionario c'è giulio
<XSickBoyX> il mio LC troverà la pass praticamente subito
<XSickBoyX> chi si vuole allenare con LC
<XSickBoyX> vi posso passare io un file SAM
<XSickBoyX> da crakkare
<XSickBoyX> ovviamente senza dirvi l'ip del sistema da dove l'ho preso :)
<XSickBoyX> cmq
<XSickBoyX> ovviamente
<XSickBoyX> il sam che vi passo io nn è facile da crakkare quindi
<XSickBoyX> nn vi aspettate un lavoro facile
<XSickBoyX> quando c'è una parola del tipo *missing*
<XSickBoyX> al posto di una pass
<XSickBoyX> vuol dire ovviamente che la pass è vuota
<XSickBoyX> x chi ama
<XSickBoyX> la riga di comando
<XSickBoyX> c'è la versione 1.5
<XSickBoyX> sul sito di Lopht
<XSickBoyX> in riga
<XSickBoyX> si chiama LC_CLI.EXE
<XSickBoyX> www.atstake.com/research/lc3/index.html
<XSickBoyX> raga secondo me un cracker di pass
<XSickBoyX> è indispensabile
<XSickBoyX> mettiamo LC da parte
<XSickBoyX> e parliamo del famosissimo John The Ripper
<XSickBoyX> anche se brevemente
<XSickBoyX> John sostanzialmente usa un dizionario
<XSickBoyX> si scarica su
<XSickBoyX> http://www.false.come/security/john
<XSickBoyX> questo è a riga di comando
<XSickBoyX> concepito x decifrare pass Unix
<XSickBoyX> ma può essere utilizzato anche per le hash di LanManager di NT

<XSickBoyX> è multipiattaforma
<XSickBoyX> è rapido (ESTREMAMENTE RAPIDO)
<XSickBoyX> e GRATUITO!
<XSickBoyX> purtroppo
<XSickBoyX> JTR
<XSickBoyX> nn riconosce la differenza tra caratteri piccoli o grandi
<XSickBoyX> ed è un casotto
<XSickBoyX> usarlo
<XSickBoyX> brevemente
<XSickBoyX> parlo anche di Crack 5
<XSickBoyX> http://www.atstake.com/products/lc/application/lc4setup.exe
<XSickBoyX> SEGNALATO DA COOL
<XSickBoyX> io vi ho dato il sito
<XSickBoyX> solo x indirizzarvi
<XSickBoyX> precisamente è qui
<XSickBoyX> GRAZIE COOL!
<XSickBoyX> cmq
<XSickBoyX> Crack
<XSickBoyX> scritto da alec Muffer
<XSickBoyX> Muffet
<XSickBoyX> era uno strumento solo x le pass di unix
<Ripper> • sick mi dicono che l'url a jtr nn funziona...
<XSickBoyX> cmq sono disponibili estenzioni
<XSickBoyX> JTR??
<XSickBoyX> un sec
<XSickBoyX> http://www.false.com/security/john
<XSickBoyX> http://www.openwall.com/john/
<XSickBoyX> avevo scritto www.false.come
<Ripper> http://www.false.com/security/john <---- era solo che avevi messo .come al posto che .com
<Ripper> grazie neso
<Ripper> scusate andiamo avanti
<XSickBoyX> appunto
<Ripper> grazie agp
<XSickBoyX> USATE QUESTO LINK
<XSickBoyX> http://www.openwall.com/john/
<XSickBoyX> questo funziona
<XSickBoyX> cmq..
<XSickBoyX> parlavo di Crack di Muffet
<XSickBoyX> questo progr
<XSickBoyX> Spero sia falso...
<XSickBoyX> cmq continuo
<XSickBoyX> allora
<XSickBoyX> Abbiamo parlato di LC
<XSickBoyX> di JTR
<XSickBoyX> e di crack5
<XSickBoyX> facciamo il caso che avete preso il sam
<XSickBoyX> e l'avete crakkato
<XSickBoyX> (vi ho spiegato come fare)
<XSickBoyX> Anzi un attimo
<XSickBoyX> qualche domanda?????
<XSickBoyX> SE AVETE DOMANDE
<XSickBoyX> QUERATE RIPPER
<Ripper> andate avanti
<Ripper> vai nn andate scusa :)
<XSickBoyX> ok andiamo avanti
<XSickBoyX> un attimo
<XSickBoyX> c'è una domanda???
<EthanHunt> scusate
<EthanHunt> posso?
<EthanHunt> ok
<EthanHunt> raga
<EthanHunt> è meglio chiarire
<EthanHunt> x chi ascolta
<EthanHunt> che cos'è
<EthanHunt> syskey e cosa NTLM
<EthanHunt> e inoltre syskey
<EthanHunt> nn è una funzione

<EthanHunt> a voi la parola
<XSickBoyX> allora
<XSickBoyX> dicevo
<XSickBoyX> la diff tra LanManager
<XSickBoyX> e SysKey
<XSickBoyX> sta nei log della scorsa lezione
<XSickBoyX> e mi pare di averla trattata abbastanza
<XSickBoyX> x quanto riguarda la parola funzione
<XSickBoyX> attribuita a SysKey
<XSickBoyX> ti dò ragione non è una funzione
<XSickBoyX> errore mio
<XSickBoyX> è una funzione di CIFRATURA
<XSickBoyX> pardon
<XSickBoyX> e come dicemmo la scorsa volta
<XSickBoyX> è una funzione
<XSickBoyX> di cifratura
<XSickBoyX> che protegge
<XSickBoyX> il reg di config
<XSickBoyX> andiamo avanti
<XSickBoyX> altre domande/critiche/consigli o altro?
<EthanHunt> posso?
<XSickBoyX> un attimo
<AGP> volevo chiedere a SickBoy....mettendo che ho il file SAM sul mio PC e lo cracco con LC o JTR o con un qualsiasi programma...quanto ci vorrà in media per beccarlo? tipo una password di media difficoltà...
<AGP> nel senso...si tratta di ore, giorni, settimana o mesi?
<XSickBoyX> matrix agp e ethanhunt
<XSickBoyX> beh AGP
<XSickBoyX> dipende dalla pass come è scritta
<XSickBoyX> tipo un qualcosa come /(£)=%&"//"?%£"£
<XSickBoyX> (ESEMPIO STUPIDO!!!!!!!!!!!!!!!!!!!!!)
<EthanHunt> allora
<EthanHunt> x pass
<XSickBoyX> e dipende anche dal tuo pc
<EthanHunt> io personalmente
<SaNdStOrM> mission impossible :-)
<EthanHunt> consiglio
<XSickBoyX> vai ethan
<XSickBoyX> dopo matrix
<EthanHunt> una pass di 7 caratteri
<EthanHunt> alfanumerica
<XSickBoyX> altro AGP?
<AGP> questo lo so...io mi chiedevo...IN MEDIA...cioè una password tipo "ciccio"
<EthanHunt> tipo d3funt0
<EthanHunt> così
<XSickBoyX> ciccio subito tramite un dizionario
<EthanHunt> visto che gli hash
<XSickBoyX> ascolta ethan....
<EthanHunt> dividono la pass
<XSickBoyX> continua
<EthanHunt> in 2 blocchi
<AGP> ecco con subito cosa intendi sick?
<EthanHunt> ognuno da 7 caratteri
<EthanHunt> quindi
<XSickBoyX> 5 min
<XSickBoyX> :)
<EthanHunt> o pass di 7
<EthanHunt> o di 14
<EthanHunt> altrimenti
<AGP> ok grazie! :-)
<EthanHunt> si rischia
<EthanHunt> di facilitare il compito
<EthanHunt> a un malicious
<tia86> + di 14 lanmanager le taglia ;)
<EthanHunt> tia86
<EthanHunt> le pass
<EthanHunt> vengono tagliate ogni 7
<EthanHunt> quindi

<EthanHunt> multipli di 7 x le pass
<EthanHunt> inoltre
<EthanHunt> vorrei dire anche un'altra cosa
<tia86> no, 2 blokki da 7, massimo totale 14 ;)
<EthanHunt> si ok su questo tia86
<EthanHunt> :D
<XSickBoyX> ethan oltre 14 nn va
<EthanHunt> il syskey
<EthanHunt> si si XSickBoyX
<EthanHunt> ok
<EthanHunt> chiudiamo quello
<EthanHunt> ok!?
<EthanHunt> allora
<EthanHunt> x syskey
<EthanHunt> in 2k
<EthanHunt> nn è presente di default
<EthanHunt> ma solo dopo il primo
<EthanHunt> service pack
<XSickBoyX> è introdotto con il service pack 2
<EthanHunt> ops
<EthanHunt> 2
<EthanHunt> :D
<XSickBoyX> il 2
<EthanHunt> c,q
<XSickBoyX> vai vai
<EthanHunt> cmq
<EthanHunt> è possibile disabilitare la syskey
<tia86> no
<EthanHunt> anche quando è attiva
<EthanHunt> se nn ci sono le adeguate
<XSickBoyX> come?
<EthanHunt> restrizioni
<EthanHunt> in alcuni valori del registro
<XSickBoyX> allora ethan
<XSickBoyX> adscusa
<XSickBoyX> se ti interrompo
<EthanHunt> vai vai
<XSickBoyX> ok
<XSickBoyX> allora
<XSickBoyX> prima di cominciare la lezione
<XSickBoyX> ho specificato che parlavamo di WinNT
<XSickBoyX> e
<XSickBoyX> se mi dai un sec
<XSickBoyX> parliamo di SySKey
<XSickBoyX> perchè ho controllato i Log
<fred`> cmq vorrei dire che il massimo di una passwd linux/unix è 8 caratteri
<XSickBoyX> e nn ne ho parlato così bene :)
<XSickBoyX> ok?
<EthanHunt> ok
<XSickBoyX> fred
<XSickBoyX> c'è una particolarità di una pass Unix di 8 caratteri???
<XSickBoyX> fred STIAMO PARLANDO DI OS UNIX-LIKE?
<XSickBoyX> cmq.....
<XSickBoyX> domande????
<EthanHunt> nn sapevo che fosse gruviera NT l'argomento
<EthanHunt> avevo chiesto a ripper
<EthanHunt> e mi aveva detto 2000
<EthanHunt> io nn ne ho altre x il momento
<XSickBoyX> No è NT
<XSickBoyX> 2000 sarà il prox
<XSickBoyX> OS che tratteremo
<XSickBoyX> CMQ
<Ripper> si sick ho cannato io scusa....
<Ripper> mi ero perso tra mille pvt
<XSickBoyX> ANdiamo avanti e parliamo appunto della punzionalità di
potenziamento della cifratura SysKey
<XSickBoyX> Ripper ci sono domande?
<XSickBoyX> parla

<Virus1986> 'sera
<Ripper> no...
<Virus1986> humm ... nulla io sapevo che il trucchetto del sam non fungeva dappertutto
<XSickBoyX> quale trukketto?
<Virus1986> Ripper sto parlando su subseven? ... quello lo usi te dopo ... semmai!
<Virus1986> XSickBoyX le psw tramite file sam
<Ripper> virus nn era riferito a te... :(
<XSickBoyX> si parla
<Virus1986> ... ugualmente ...
<XSickBoyX> ripper nn si riferiva a te
<XSickBoyX> continua
<Virus1986> (22:44:20) (+Virus1986) XSickBoyX le psw tramite file sam
<XSickBoyX> si
<Virus1986> non sempre funziona ...
<Virus1986> in che casi nn funge =?
<XSickBoyX> continuo a non capire
<XSickBoyX> cosa nn funziona??
<XSickBoyX> i metodi x prendere il SAM
<XSickBoyX> o il crack del SAM?
<Virus1986> clap clap esatto
<Virus1986> i metodi per prendere il sam
<XSickBoyX> virus cazzo STO PARLANDO DEL CRACK
<XSickBoyX> DEI METODI NE HO PARLATO X DUE LEZIONI!!!
<Virus1986> embè ...
<Virus1986> io ho scoperto solo oggi
<XSickBoyX> hai letto i log???
<Virus1986> questo magnifico canale
<XSickBoyX> ok
<XSickBoyX> a quale metodo ti riferisci?
<XSickBoyX> il reboot
<XSickBoyX> lo sniffing
<Virus1986> che sam latecnica del sam codda ?
<XSickBoyX> quello del repair
<XSickBoyX> o il dll injection?
<Virus1986> l'ignezione delle dll
<XSickBoyX> CHE VUOL DIRE SCUSA LA DOMANDA "CHE SAM LATECNICA DEL SAM CODDA????"
<XSickBoyX> ok
<Ripper> <EthanHunt> penso inoltre
<Ripper> <EthanHunt> che vada aggiunto
<Ripper> <EthanHunt> il fatto
<Ripper> <EthanHunt> che si parla di SAM
<Ripper> <EthanHunt> solo se il pc
<Ripper> <EthanHunt> nn è un controller di dominio
<Ripper> <EthanHunt> un domain controlle
<XSickBoyX> si
<XSickBoyX> lo dissi
<XSickBoyX> due lezioni fa
<XSickBoyX> ethan
<XSickBoyX> io ogni lunedi sto qui e lavoro
<XSickBoyX> ed io rispetto tutti
<[M]atriX> io vorrei porre il seguente quesito:
<XSickBoyX> ma rispettate anche me..
<XSickBoyX> vai
<[M]atriX> Non avendo i privilegi admin e volendo prelevare il file sam quali strada m si aprono (nb. è la prima lezione che seguo).
<XSickBoyX> dovresti trovare alcune tecniche neelle lezioni passate
<[M]atriX> si ovviamente
<[M]atriX> m ha particolarmente stupito la tecnica sam codda
<XSickBoyX> ma cmq ne parleremo completanto il discorso SU NT/2000 in modo da chiudere completamente il discorso WINZOZZ OS!
<[M]atriX> io onestamente la conosco per sentito dire
<[M]atriX> vuoi me ne potete dare una delucidazione?
<XSickBoyX> ETHAN ti apprezzo tantissimo che partecipi
<XSickBoyX> e mi fa piacere
<XSickBoyX> chee sei attivo
<EthanHunt> grazie

<XSickBoyX> scusa se hai pensato che ti mancassi di rispetto o che ho pekkato di arroganza.....
<EthanHunt> XSickBoyX
<EthanHunt> tutto ok
<XSickBoyX> nn erano le mie intenzioni... seriamente
<EthanHunt> chiarito
<[M]atriX> ...
<EthanHunt> ok ok
<EthanHunt> ci sono rimasto di merda
<EthanHunt> un'altra così e me ne vado
<EthanHunt> ok?
<EthanHunt> toglietemi il voice
<XSickBoyX> matrix nn conosco la tecnica "sam codda"
<XSickBoyX> ,,,,,,,
<XSickBoyX> andiamo avanti
<Ripper> andiamo avanti va che è meglio
<XSickBoyX> appunto
<XSickBoyX> stasera....
<XSickBoyX> ehehehe è da uscire pazzi :)
<XSickBoyX> ethan altro da dire??
<XSickBoyX> vabbè
<XSickBoyX> cmq
<XSickBoyX> una volta che abbiamo finalmente le credenziali ADMIN
<XSickBoyX> NN ABBIAMO l'intero dominio
<XSickBoyX> come facciamo ad espandere il nostro potere?
<XSickBoyX> beh innanzitutto
<XSickBoyX> molti admin
<XSickBoyX> usano le stesse pass
<XSickBoyX> x l'admin locale e quello di dominio
<XSickBoyX> cmq...
<XSickBoyX> facciamo un esempio di situazione tipica
<XSickBoyX> facciamo il caso
<XSickBoyX> "con molto culo"
<XSickBoyX> bekkiamo
<XSickBoyX> una makkina di test nel dominio
<XSickBoyX> pe cui la pass dell'utente locale ,che è admin, è vuota
<XSickBoyX> allora
<XSickBoyX> che accade??
<XSickBoyX> di regola
<XSickBoyX> nn dovremmo andare oltre
<XSickBoyX> perchè
<XSickBoyX> questo account
<XSickBoyX> dovrebbe essere attivo solo nel locale
<XSickBoyX> facciamo il caso
<XSickBoyX> che un admin
<XSickBoyX> abbia installato il sistema win nt di test
<XSickBoyX> e ha creato
<XSickBoyX> anche un nome utente nel dominio
<XSickBoyX> che è il duplicato del nome utente locale
<XSickBoyX> (perchè???
<XSickBoyX> semplicemente x velocizzare l'accesso alle altre risorse del dominio
<XSickBoyX> x il test
<XSickBoyX> e zack
<XSickBoyX> il tutto diventa facile
<XSickBoyX> cmq mi rendo conto
<XSickBoyX> che devo prendere sto discorso
<XSickBoyX> con un altra piega
<XSickBoyX> ma se nn avete nulla in contrario continuiamo la prox volta
Session Close: Mon Nov 10 23:25:10 2003