Session Start: Mon Oct 27 20:36:59 2003
Session Ident: #AlexMessoMalex
* Now talking in #AlexMessoMalex
* Topic is '•0,2Si prega di visitare la sezione •8•FAQ••0 e il •8•FORUM••0 prima di chiedere ai moderatori.••'
* Set by SaNd|aWaY on Mon Oct 27 20:35:09
* XsickboyX has joined #AlexMessoMalex
* Figs has quit IRC (Quit: Leaving•)
<XsickboyX> vabbe
<XsickboyX> visto che
<XsickboyX> già è tardi
<XsickboyX> nn perdo altro tempo
* AlexMessoMalex sets mode: +v XsickboyX
<XsickboyX> possiamo?
<zioponch> certo
<ser16> vai
<XsickboyX> ok parto subito
<AlexMessoMalex> INIZIAMO
<DjCoNdOr> siamo a tutt'occhi
<DjCoNdOr> solo una cosa
<tiranno> vaiii
* Ripper sets mode: +m
<XsickboyX> allora
<XsickboyX> la scorsa
<XsickboyX> volta parlammo
<XsickboyX> di come si può scoprire una pass
<XsickboyX> tramite un bruceforce
<XsickboyX> o tramite la prova di pass note
<XsickboyX> e parlammo degli script for
<XsickboyX> x farci una bella routine x provare delle pass
<XsickboyX> allora
<XsickboyX> oggi parlleremo dei buffer overflow
<XsickboyX> di cosa sono
<XsickboyX> come si usano ect
<XsickboyX> allora
<XsickboyX> circola
<XsickboyX> una leggenda metropolitana
<XsickboyX> in internet
<XsickboyX> che dice che alcuni bug
<XsickboyX> di alcune applicazioni di Win nt
<XsickboyX> dovrebbe consentire
<XsickboyX> l'accesso root in remoto
<XsickboyX> in realtà
<XsickboyX> è che solo
<XsickboyX> in pochissimi casi sta cosa è stata provata
<XsickboyX> cmq
<XsickboyX> uno dei più temuti difetti è appunto sto buffer overflow
<XsickboyX> i problemi
<XsickboyX> relativi del Buffer overflow
<XsickboyX> si presentano quando le applicazioni
<XsickboyX> nn controllano la lunghezza di un input
<XsickboyX> se
<XsickboyX> si sfrutta un errore del genere ad hoc
<XsickboyX> si possono avviare programmi da remoto
<XsickboyX> il che è na grande cosa
<XsickboyX> ho fatto una ricerca
<XsickboyX> e sarebbe buono leggere
<XsickboyX> il num 49 di phrack
<XsickboyX> http:\\phrack.org
<XsickboyX> l'articolo "smashing the stack for fun and profit"
<XsickboyX> da leggere
<XsickboyX> cmq
<XsickboyX> i buffer overflow
<XsickboyX> si suddividono in due parti
<XsickboyX> REMOTO E LOCALE
<XsickboyX> i locali richiedono l'accesso via console all'exploit e in genere

sono disponibili se gli utenti sono collegati
<XsickboyX> in maniera interattiva
<XsickboyX> i remoti
<XsickboyX> sono molto più pericolosi
<XsickboyX> xkè possono essere lanciati
<XsickboyX> senza privilegi
<XsickboyX> e da qualunque nodo della rete
<XsickboyX> vi descrtivo brevemente alcuni uffer overflow
<XsickboyX> che copnosco
<XsickboyX> :)
<XsickboyX> Allora
<XsickboyX> ISSHACK
<XsickboyX> o quello che colpisce l'oracle web listener
<XsickboyX> o quello chwe sfrutta
<XsickboyX> outlook
<XsickboyX> insomma ce ne sono tanti
<XsickboyX> stavo pensando di fare una lezione a parte sui BO
<XsickboyX> no vabbè
<XsickboyX> andiamo avanti
<XsickboyX> completeremo il discorso dei BO in un 'altra lezione
<XsickboyX> adesso accenniamo cosa sono i denial of service
<XsickboyX> cioè rifiuto di servizio
<XsickboyX> perchè sto parlando superficialmente di questi attakki?
<XsickboyX> perchè
<XsickboyX> fanno parte dei sistemi NT
<XsickboyX> e cmq ne parleremo quando faremo hacking avanzato
<XsickboyX> allora
<XsickboyX> gli attakki DoS
<XsickboyX> hanno avuto il loro boom
<XsickboyX> quando si misero alla luce diversi bachi
<XsickboyX> che permettevano di inviare
<XsickboyX> pakketti TCP/IP anomali
<XsickboyX> oggi ahime
<XsickboyX> è usato poco il DoS
<XsickboyX> sia perchè la maggior parte
<XsickboyX> sono stati risolti
<SaNdStOrM> sxdfhgjsh, usa il tuo vero nick, tanto non sei nell'akick
<XsickboyX> sia perchè non sono considerati "elite"
<XsickboyX> anche se possono essere usati per provocare
<XsickboyX> riavvii di sistema forzati
<XsickboyX> allora
<XsickboyX> cambiando discorso
<XsickboyX> ultimamente
<XsickboyX> ho avuto a che fare con tante persone che facevano attakki
<XsickboyX> usando il baco unicode di IIS
<XsickboyX> con vari scanner ect
<XsickboyX> molte persone però
<XsickboyX> si fermano a installare netcat
<XsickboyX> (nc.exe)
<XsickboyX> che alla fine funge da backdoor
<XsickboyX> x avere un accesso
<XsickboyX> via telnet
<XsickboyX> da qui volevo aprire il discorso sul SAM
<XsickboyX> Security Account Manager
<XsickboyX> ma ne parleremo fra un pò
<XsickboyX> se abbiamo un account
<XsickboyX> valido ma nn admin
<XsickboyX> l'unica speranza
<XsickboyX> è cercare
<XsickboyX> di aumentare i propri privilegi
<XsickboyX> come fare?
<XsickboyX> RICERCA RICERCA RICERCA
<XsickboyX> allora
<XsickboyX> potremmo usare Legion o srvinfo nel NTRK (NT ROOT KIT)
<XsickboyX> che cerca condivisioni
<XsickboyX> tipo systemroot\system32
<XsickboyX> o \repair
<XsickboyX> a che serve?

<XsickboyX> in repair c'è la copia di backup del SAM
<XsickboyX> ma andiamo con ordine
<XsickboyX> una volta
<XsickboyX> connessi
<XsickboyX> con
<XsickboyX> il vostro account
<XsickboyX> (che avete trovato ovviamente)
<XsickboyX> e aver fatto le appropriate ricerce
<XsickboyX> proviamo qualche attakko stupido, obsoleto ma a volte efficace
<XsickboyX> esiste un programmino
<XsickboyX> chiamato getadmin
<XsickboyX> che tenta
<XsickboyX> di aggiungere il vostro account
<XsickboyX> nel gruppo admin
<AlexMessoMalex> •11,2facciamo una pausa domande
<XsickboyX> sfruttando una procedura a basso livello del kernel di winzozz
<XsickboyX> un sec
<XsickboyX> alex
<XsickboyX> termino
<AlexMessoMalex> ok, un sec
<XsickboyX> su get admin
<XsickboyX> ASPE
<XsickboyX> finisco su get admin
<XsickboyX> e poi domande
<XsickboyX> dopo
<XsickboyX> aver provato get admin
<XsickboyX> si può usare
<XsickboyX> una tecnica chiamata dll injection
<XsickboyX> che consente l'inserimento
<XsickboyX> e l'esecuzione di codice
<XsickboyX> di propria scelta all'interno
<XsickboyX> di un processo che ha il privilegio
<XsickboyX> e la possibilità di aggiungere utenti
<XsickboyX> al gruppo administrators
<XsickboyX> (x la cronaca il processo alterato sarà il winlogon)
<XsickboyX> qual'è il problema
<XsickboyX> di getadmin?
<XsickboyX> è che dev'essere avviato
<XsickboyX> su un sistema locale
<XsickboyX> sul sistema remoto i
<XsickboyX> pardon
<XsickboyX> ovviamente
<XsickboyX> i gruppi "normali " nn possono accedere alla console di sistema
<XsickboyX> quindi dovremmo avere un account di tipo
<XsickboyX> Server
<XsickboyX> cioè
<XsickboyX> admin
<XsickboyX> ma
<XsickboyX> se avete l'accesso admin
<XsickboyX> che ve ne fate di un altro admin???
<XsickboyX>  :)
<XsickboyX> magari come backdoor
<XsickboyX> cmq
<XsickboyX> getadmin
<XsickboyX> viene avviato con la seguente grammatica
<XsickboyX> GETADMIN NOME_UTENTE
<XsickboyX> e zack
<XsickboyX> siamo admin
<XsickboyX> se volete vedere se il programma funzionerà
<XsickboyX> senza
<XsickboyX> creare casini
<XsickboyX> provate ad avviare windisk
<XsickboyX> o programmi del genere
<XsickboyX> che sono avviabili
<XsickboyX> dal solo admin
<XsickboyX> adesso
<XsickboyX> potete fare domande
<DjCoNdOr> sick

<sxdfhgjsh> posso?
<zioponch> sick io vorrei cominciare dal'inizio dall'overflow
<Ripper> fermi fermi
<XsickboyX> uno alla volta
<XsickboyX> vai condor
<Ripper> facciamo
<Ripper> cosi
<Ripper> diamo il +v
<Ripper> a tot persoen
<Ripper> persone altrimenti...
<XsickboyX> chiamate in pvt ripper che vi da il voice
<XsickboyX> ripper
<XsickboyX> dai il voice
<XsickboyX> a chi deve fare domande
<XsickboyX> chiamate ripper lui dà il voice
<XsickboyX> ect
<XsickboyX> dimmi
<DjCoNdOr> sisick
<DjCoNdOr> io ho un problema
<XsickboyX> tante persone hanno problemi :)
<XsickboyX> dimmi
<DjCoNdOr> con xp non funziona?
<XsickboyX> cosa?
<DjCoNdOr> l'overflow
<XsickboyX> lanciarlo o riceverlo?
<DjCoNdOr> lanciarlo
<XsickboyX> non conosco bene xp
<XsickboyX> ma dovrebbe lancialro
<DjCoNdOr> mannaia
<DjCoNdOr> io ho xp
<DjCoNdOr> e nonstante seguo le lezioni
<DjCoNdOr> non riesco a fare le prove
<DjCoNdOr> per alcune funzioni diverse
<XsickboyX> consiglio personale
<XsickboyX> xp è un buon OS
<XsickboyX> x l'utente
<XsickboyX> a cui nn interessano
<XsickboyX> ste cose
<XsickboyX> o passate a linux
<XsickboyX> o a win 2000
<DjCoNdOr> lo so
<DjCoNdOr> benissimo
<DjCoNdOr> infatti ho intenzione di provare con linux
<XsickboyX> cmq
<Ripper> ok direi di passare al prossimo
<DjCoNdOr> allora non mi puoi aiutare per questa cosa
<DjCoNdOr> vapito
<XsickboyX> utilizza la mandrake
<XsickboyX> condor
<XsickboyX> non mi hai fatto una domanda precisa
<sxdfhgjsh> grazie
<sxdfhgjsh> la domanda:
<sxdfhgjsh> se per diventare admin devo lanciare un programma che richiede accesso admin, a che serve?
<sxdfhgjsh> sarei già admin
<XsickboyX> appunto
<XsickboyX> l'ho già detto
<sxdfhgjsh> senza fare tutto quel macello
<XsickboyX> io
<XsickboyX> lo puoi usare
<XsickboyX> per creare una backdoor
<XsickboyX> cioè un account
<sxdfhgjsh> a che serve?
<XsickboyX> con cui rientrare
<XsickboyX> quando fai il log
<XsickboyX> pardon
<XsickboyX> il log in
<XsickboyX> viene segnalato

<XsickboyX> cioè
<XsickboyX> c'è data e ora dell'ultima connessione admin
<XsickboyX> se l'utente admin
<XsickboyX> nn si connette da un mese
<XsickboyX> mentre tu lo fai col suo account ogni giorno
<XsickboyX> beh
<XsickboyX> ti fai sgamare
<XsickboyX> avuto l'utente admin
<sxdfhgjsh> e si
<XsickboyX> nn ti conviene usarlo
<XsickboyX> spesso
<XsickboyX> anzi meglio usare altre tecniche
<sxdfhgjsh> però nn si vede quali account sono di tipo admin?
<XsickboyX> come winvnc
<XsickboyX> si
<sxdfhgjsh> di regola solo uno dovrebbe essere di quel tipo
<XsickboyX> ahime
<XsickboyX> no
<XsickboyX> questo nn è detto
<XsickboyX> xò
<XsickboyX> ho spiegato sta cosa
<XsickboyX> xkè esiste
<XsickboyX> :)
<XsickboyX> cioè
<XsickboyX> se qualcuno ha questo tipo di bisogno deve saperlo fare :)
<sxdfhgjsh> capisco
<XsickboyX> e getadmin
<XsickboyX> lo fa facilmente
<sxdfhgjsh> grazie mille
<XsickboyX> di nulla
<Ripper> a posto sxdfhgjsh ??
<XsickboyX> Il prossimo grazie
<sxdfhgjsh> si, grazie
<XsickboyX> : ) mi sento un dottore
<sxdfhgjsh> mi fa male il pisello
<XsickboyX> eheheh
<zioponch> posso?
<XsickboyX> x quello vai da na puttana
<XsickboyX> prezgo
<XsickboyX> prego
<XsickboyX> sxdfhgjsh DEVI SCOPARE
<XsickboyX> :)
<zioponch> allora io vorrei se possibile avere un esempio di cosa comporta l'overflow
<XsickboyX> esempio pratico
<XsickboyX> se un programma è settato
<XsickboyX> x ricevere
<XsickboyX> un numero di due caratteri
<XsickboyX> e nn sa come comportarsi
<XsickboyX> se riceve un num di tre
<XsickboyX> allora si ingrippa
<XsickboyX> e tu puoi sfruttare sta cosa
<XsickboyX> ovviamente ci sono dei Buffer Overflow conosciuti
<XsickboyX> perchè la maggior parte delle volte l'applicazione
<XsickboyX> va in crash insieme alla makkina
<XsickboyX> alcune volte però
<XsickboyX> questo crash
<zioponch> e come faccio a capirlo se ci sono sti buffer overflow sconosciuti in una applicazione?
<XsickboyX> beh zio ponch facile
<zioponch> o macchina?
<XsickboyX> se conosci BENE qualche applicazione
<XsickboyX> puoi provare ad inserire un input "sballato"
<XsickboyX> e vedere che succede
<zioponch> tipo?
<XsickboyX> magari trovi qualcosa di interessant
<XsickboyX> e che ne so
<XsickboyX> se lo sapevo lo facevo io no?

<XsickboyX> :)
<zioponch> scusa
<XsickboyX> ehehehehehh
<XsickboyX> www.cerberus-infosec.co.uk/
<XsickboyX> trovate tante info su tanti buffer overflow
<XsickboyX> conosciuti
<XsickboyX> prendete spunto da lì
<Ripper> google è il nostro miglior amico  :)
<XsickboyX> mi spiace ammettere che nn ho mai scoperto un buffer overflow
<XsickboyX> ho fatto delle ricerche su alcuni argomenti
<XsickboyX> visto che nn posso spiegare tutti
<XsickboyX> tutto
<XsickboyX> vi dò degli spunti
<XsickboyX> su cui guardare :)
<zioponch> ok
<Ripper> a posto zioponch  ???
<zioponch> no ancora 2 cose
<zioponch> se posso
<Ripper> vai tutto tuo... rapido però
<zioponch> una riguarda il DoS e l'altra quello che spiegavi sul fatto di avere l'accesso adin
<XsickboyX> si il getadmin
<XsickboyX> (ci sono altri metodi)
<zioponch> admin sorry
<XsickboyX> fa nulla continua
<XsickboyX> dimmi
<XsickboyX> la prima
<XsickboyX> es il NetStrike è un DoS
<XsickboyX> cioè
<zioponch> il DoS a che scopo potrei utilizzarlo e come trovare gli ISS?
<XsickboyX> no aspè
<XsickboyX> il dos nn è solo su gli IIS
<zioponch> ahh
<XsickboyX> il dos
<XsickboyX> può essere utilizzato x FAR RIAVVIARE UNA MAKKINA
<XsickboyX> esempio pratico
<XsickboyX> facciamo il caso
<XsickboyX> che abbiamo messo
<XsickboyX> il server di un trojan
<XsickboyX> nella cartella di esecuzione automatica
<XsickboyX> cerchiamo di far crashare
<XsickboyX> il pc vittima
<XsickboyX> eseguendo un dos
<XsickboyX> o facciamo il caso
<XsickboyX> che vogliamo oscurare" un sito
<XsickboyX> facciamo un dos di tipo flooding
<zioponch> cioè?
<XsickboyX> mai sentito parlare di NetStrike?
<XsickboyX> netstrike = cyber manifestazione
<XsickboyX> alcuni gruppi
<zioponch> no purtroppo è da poco che mi interesso e so poco..ma cerco di imparare
<XsickboyX> si
<XsickboyX> organizzano
<XsickboyX> in modo tale
<XsickboyX> da connettersi insieme nello stesso momento ad un sito
<XsickboyX> poi tutti
<zioponch> e quindi farlo cadere?
<XsickboyX> si connettono si sconnettono e si riconnettono
<XsickboyX> finchè
<XsickboyX> quel sito collassa
<XsickboyX> e si opscura
<Ripper> zioponch nn posso + tenere moderato il canale... rapidizzati...
<zioponch> x quel periodo fino a che il server riparte vero?
<XsickboyX> questo è un esempio di DoS (Denial Of Service ossia negazione di servizio)
<XsickboyX> terza domanda
<XsickboyX> sull'admin

<XsickboyX> veloce
<zioponch> ok l'ultima vcosa
<zioponch> il fatto di aver un accesso admin in una macchina a cosa serve?
<XsickboyX> AZZ
<XsickboyX> SEI PRATICAMENTE IL PADRETERNO!
<XsickboyX> hai il pc nelle tue mani
<Ripper> admin = administrator = amministratore
<zioponch> ma il fatto del locale e emoto?
<zioponch> remoto ops
<XsickboyX> zio ponch
<XsickboyX> x farti capire
<XsickboyX> tu sei admin del tuo pc
<zioponch> si
<XsickboyX> essere admin vuol dire avere il nome utente e la pass di un altro pc
<zioponch> ma a me serve averne un altro x nn far apparire nei log che ci sono entrato??
<XsickboyX> zio ponch
<XsickboyX> il discorso è troppo lungo
<zioponch> ok
<XsickboyX> x essere fatto qui
<XsickboyX> leggi le mie guide
<zioponch> mi spieghera un atro
<XsickboyX> e i log
<zioponch> dove le trovo le guide?
<XsickboyX> sul sito di alex
<zioponch> ok
<zioponch> si potrebbe chiedere una cosa che nn centra?
<XsickboyX> ehehehe
<XsickboyX> altre domande???
<XsickboyX> oltre sta cosa che nn c'entra?
<Ripper> ----- ci sono altre domande ??? -------------
<Ripper> in pvt please
<Ripper> sick vuoi continuare ??
<XsickboyX> ok continuaio
<XsickboyX> allora
<XsickboyX> vorrei parlare di secholed
<XsickboyX> ma visto che è simile
<XsickboyX> a getadmin
<XsickboyX> nn vene parlo
<XsickboyX> ma dico solo una cosa su secholed
<XsickboyX> secholed
<XsickboyX> in alcuni casi
<XsickboyX> si può avviare in remoto
<XsickboyX> come fare?
<XsickboyX> spesso e volentieri su sitemi Nt
<XsickboyX> ci sono directory dove sono attivi diritti di scrittura e lettura
<XsickboyX> messi a disposizione da IIS
<XsickboyX> le dir virtuali messe a disposizione da IIS
<XsickboyX> sono tutte contrassegnate come eseguibili dal server di web
<XsickboyX> in base a ste cose
<XsickboyX> chiunque
<XsickboyX> può copiare
<XsickboyX> secholed
<XsickboyX> lì
<XsickboyX> e ottenere l'admin da remoto
<XsickboyX> l'unico casino
<XsickboyX> è copiare il programma in una di queste dir (che dirò dopo quali sono)
<XsickboyX> vi dico qualche via d'entrata
<XsickboyX> condivisioni di unità
<XsickboyX> senza pass
<XsickboyX> dir FTP con privilegidi root
<XsickboyX> shell di comando remote
<XsickboyX> non protette ovviamente
<XsickboyX> telnet
<XsickboyX> o addirittura alcune funzioni di frontpage
<XsickboyX> e cmq una volta
<XsickboyX> trovato un modo x caricare codice

<XsickboyX> avviare codice
<XsickboyX> è facile
<XsickboyX> trovare un modo x copiare un file
<XsickboyX> (può bastare anche una email)
<XsickboyX> facciamo il caso
<XsickboyX> che troviate il modo
<XsickboyX> x caricare secholed e le sue dll
<XsickboyX> visto che secholed
<XsickboyX> dev'essere avviata da una shell
<XsickboyX> di comando
<XsickboyX> possiamo usare
<XsickboyX> cmd.exe
<XsickboyX> cioè l'interprete dei comandi di NT
<XsickboyX> che si trova su sistemroot\system32
<XsickboyX> possiamo
<XsickboyX> anche fare una cosa più carina
<XsickboyX> possiamo
<XsickboyX> fare un file .bat
<XsickboyX> dal nome innocuo e avviarlo
<XsickboyX> da remoto
<XsickboyX> e che ci scriviamo nel bat?
<XsickboyX> questo
<XsickboyX> net user nomeutente password /add && net localgroup administrators nomeutente /add
<XsickboyX> avviamo in questo modo
<XsickboyX> http://nomesito.com/nomedirectory(le dico dopo,in questo caso scripts)/cmd.exe?c%20c:\inetpub\(nome dir)\nomefile.bat
<XsickboyX> allora
<XsickboyX> il file cmd.exe sta nella dir scripts
<XsickboyX> adesso andiamo a vedere quelle dir di iis dove possiamo caricare i files
<XsickboyX> allora
<XsickboyX> la prima voce
<XsickboyX> è la dir virtuale
<XsickboyX> la seconda è la reale locazione sul HD
<XsickboyX> root/news    c:\inetpub\News
<XsickboyX> root/mail          c:\inetpub\mail
<XsickboyX> root/cgi-bin            c:\inetpub\wwwroot\cgi-bin
<XsickboyX> root/scripts               c:\inetpub\scripts
<XsickboyX> queste conosco
<XsickboyX> ma penso ce ne siano altre
<XsickboyX> cmq
<XsickboyX> nell'url
<XsickboyX> x avviare il file but
<XsickboyX> bat
<XsickboyX> il 520 è semplicemente uno spazio
<XsickboyX> domande???
<zioponch> si può?
<N_E_S_O> •.
<XsickboyX> si
<XsickboyX> ULTIMA COSA
<zioponch> ok
<XsickboyX> la lezione finisce qui
<XsickboyX> siamo in pochi
<XsickboyX> e s'è fatto tardi
<XsickboyX> causa il mio ritardo come al solito
<XsickboyX> DOMANI SERA ORE 21
<XsickboyX> PROX LEZIONE