Session Start: Tue Oct 28 20:45:40 2003
Session Ident: #AlexMessoMalex
* Now talking in #AlexMessoMalex
* Topic is '•8,10•www.AlexMessoMalex.com Prossima lezione •4,15•QUESTA SERA•• ore 21.30 •••0,2 Si prega di visitare la sezione •8•FAQ••0 e il •8•FORUM••0 prima di chiedere ai moderatori.••'
* Set by AlexMessoAway on Tue Oct 28 12:16:53

<XsickboyX> ciao a tutti
<XsickboyX> allora
<XsickboyX> dobbiamo terminare il discorso di secholed e get admin
<XsickboyX> chi ha seguito ieri SPERO ricorda
<XsickboyX> cosa sono secholed e getadmin
<XsickboyX> brevemente sono programmi che, se avviati con privilegi root, aggiungono un nick
<XsickboyX> nel gruppo administrators
<XsickboyX> per la cronaca stiamo parlando di win nt :)
<XsickboyX> X copletare sto discorso
<XsickboyX> vi dò le chiavi di registro
<XsickboyX> che avviano automaticamente files all'avvio del sistema
<XsickboyX> Allora
<XsickboyX> HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
<XsickboyX> hklm\ect...ect...ect\CurrentVersion\RunOnce
<XsickboyX> HKLM\ect ect ect\CurrentVersion\RunOnceEx
<XsickboyX> HKLM\Software\microsoft\WindowsNT\CurrentVersion\AeDebug
<XsickboyX> HKLM\Software\Microsoft\WindowsNT\CurrentVersion\WinLogon
<XsickboyX> queste sono quelle che conosco
<XsickboyX> Adesso FINALMENTE
<XsickboyX> parliamo del simpaticissimo e meraviglioso SAM
<XsickboyX> Security Account Manager
<XsickboyX> no lo Zio Sam americanO!
<XsickboyX> cmq... cos'è il SAM?
<XsickboyX> è un file (senza estenzione)
<XsickboyX> equivalente al file /etc/passwd nei sistemi Linux
<XsickboyX> e praticamente un file
<XsickboyX> che contiene tutti i nomi utenti e le relative pass, cifrate,
<XsickboyX> di un sistema locale
<XsickboyX> Riuscire ad ottenere il SAM
<XsickboyX> è come avere la copia delle chiavi di un appartamento
<XsickboyX> Poco tempo fa parlammo dello sfruttamento di Unicode dell 'IIS
<XsickboyX> (lo citammo in realtà)
<XsickboyX> beh
<XsickboyX> chi ha un accesso di quel tipo
<XsickboyX> può ottenere il SAM facilmente
<XsickboyX> e cmq il SAM si deve prendere sempre...
<XsickboyX> cosa ne facciamo del SAM?
<XsickboyX> beh ne prendiamo una copia e cerchiamo di crakkarlo
<XsickboyX> ovviamente
<XsickboyX> detto "facile"
<XsickboyX> lo prendiamo e lo crakkiamo con un bruceforce tipo L0phtCrack (io uso quello)
<XsickboyX> allora
<XsickboyX> visto che L0phtCrack
<XsickboyX> ha solo un dizionario
<XsickboyX> vi consiglio di andare su http://coast.cs.purdue.edu
<XsickboyX> se date una buona okkiata (e se ci sono ancora) dovrebbero esserci dei dizionari belli e pronti
<XsickboyX> Cmq andiamo avanti
<XsickboyX> Il SAM si trova nella dir systemroot\System32\Config
<XsickboyX> ma ahimè
<XsickboyX> l'accesso a questa dir è bloccato quando l'os
<XsickboyX> è in esecuzione
<XsickboyX> come fare???
<XsickboyX> esistono 4 sistemi x prendere il SAM
<XsickboyX> 1 eseguire
<XsickboyX> il boot

<XsickboyX> del sistema con un altro sistema operativo
<XsickboyX> (xkè la dir dove sta il SAM
<XsickboyX> non è protetta con altri OS)
<XsickboyX> 2 Ottenere la copia di backup del file SAM creato dalla procedura di Windows NT Repair Disk Utility
<XsickboyX> 3 estrarre direttamente le hash delle pass dal SAM
<XsickboyX> 4 usare la tecnica del Man In The Middle
<XsickboyX> tipo la tecnica dell'SMB Capture vista qualche tempo fa
<XsickboyX> OK
<XsickboyX> prima ondata di domande
<Sbirilindo> (uomo in mezzo)
<XsickboyX> querate in privato UNO DEGLI OP
<XsickboyX> si
<XsickboyX> uno sniffer in pratica
<XsickboyX> QUERATE UNO DEGLI OP SE AVETE DOMANDE
<XsickboyX> dimmi
<XsickboyX> somebody
<Ripper> somebodyyyyyyyyyy
<XsickboyX> ???
<XsickboyX> cazzo che domandone!!
<somebody> <XsickboyX> brevemente sono programmi che, se avviati con privilegi root, aggiungono un nick <-- come avvio un programma con privilegi root in windows?
<XsickboyX> beh lo dissi ieri
<XsickboyX> sembra stupido
<somebody> ma root non l'ho mai sentito
<somebody> per quello
<XsickboyX> ma x avviare un progr con privilegi root devi avere le credenziali dell'admin
<XsickboyX> root inteso come admin
<somebody> ahh
<XsickboyX> privilegi di amministratore
<somebody> perche non ricordo di aver mai letto root
<XsickboyX> in pratica
<somebody> da nessuna parte nel mio windows
<XsickboyX> se hai l'user e la pass di un utente admin
<XsickboyX> puoi avviare un progr del genere
<XsickboyX> tu potrai chiedere a che serve??
<XsickboyX> beh a crearsi una backdoor
<somebody> a ke serve?
<XsickboyX> ieri mi chiesero
<somebody> ah
<XsickboyX> "ma l'admin nn vede che abbiamo aggiunto un nuovo account al gruppo admin??"
<XsickboyX> beh si
<XsickboyX> ma io l'ho spiegato
<XsickboyX> xchè se vi serve x qualche motivo
<XsickboyX> lo potete fare :)
<somebody> ah occhei
<XsickboyX> e poi l'admin nn controlla continuamente chi fa parte del suo gruppo
<XsickboyX> ok?
<somebody> grazie
<XsickboyX> perfetto
<XsickboyX> di nulla
<somebody> ah
<somebody> ma l'admin in poke parole
<somebody> è scemo
<XsickboyX> beh dipende che admin bekki
<XsickboyX> l'admin è praticamente il proprietario del sistema
<somebody> no ma dico: l'admin in generale è un cojone?
<XsickboyX> ci sono persone PARANOICHE
<XsickboyX> somebody ci sono tanti admin coglioni più di quanto ne pensi
<XsickboyX> vai zio
<zioponch> sick
<zioponch> io avrei soloù
<zioponch> una domanda
<XsickboyX> dimmi
<zioponch> la tecnica dell'SMB

<zioponch> in cosa consiste?
<XsickboyX> ahia..... nn c'eri??
<XsickboyX> cazz.....
<zioponch> no purtroppo
<XsickboyX> è lunga come questione e l'accennai
<zioponch> nemmeno so il man in the middle
<XsickboyX> cmq sfrutta la tecnica chiamata MAN IN THE MIDDLE
<XsickboyX> cioè uomo nel mezzo
<XsickboyX> cosa che spiegheremo più avanti
<XsickboyX> praticamente funziona così
<zioponch> ma nn conosco nemmeno man in the middle
<XsickboyX> FACCIAMO IL CASO CHE A è il sistema dell'attakkante e B è il sistema da attakkare ok???
<zioponch> ok
<XsickboyX> le autenticazioni di B vengono dirottate
<XsickboyX> verso uno sniffer
<XsickboyX> che manda le informazioni sullo user e sulla pass
<XsickboyX> al sistema A
<zioponch> -ok
<XsickboyX> e poi rimanda il SISTEMA B al sito richiesto
<XsickboyX> in modo da nn dare nell'okkio
<XsickboyX> ma lo spiegherò più in la
<Ripper> a posto ?
<XsickboyX> altre domande?
<XsickboyX> vai spax
<Ripper> spaxxxxxxx
<SPAX> xsickboyx
<SPAX> eccome
<SPAX> era una domanda vecchia
<XsickboyX> beh prova
<SPAX> ma forse hai già risposto
<SPAX> parlavi prima del sam
<XsickboyX> si
<SPAX> e hai detto di aggiungere un user administrator usando privilegi root
<SPAX> ma nno esistono gruppi o user root su wndows
<SPAX> o mi sbaglio^?
<XsickboyX> SU WIN 98/95/me ect no
<XsickboyX> ma su win XP/2000/NT si
<XsickboyX> perchè sono sistemi multiutente
<XsickboyX> come gli unix-like
<SPAX> si ma non esiste l'utente root comunque
<XsickboyX> infatti questa lezione parla SOLO di WinNT
<XsickboyX> no
<XsickboyX> esiste l'utente admin
<XsickboyX> la parola root la uso
<SPAX> nemmeno admin
<XsickboyX> x indicare i privilegi di amministratore
<SPAX> non esiste ne root ne admin
<XsickboyX> SPAX X DEFAULT su un sistema NT esiste il gruppo administrators
<XsickboyX> ti trovi?
<SPAX> scusa a questo punto chiamali toor visto che ci sei..
<SPAX> forse eri un po' impreciso..
<XsickboyX> root o admin nn sono parole che mi sono inventato
<SPAX> si administrators si
<SPAX> non admin
<XsickboyX> NN POSSO SCRIVERE administrators
<SPAX> nel mondo windows si
<SPAX> te le sei inventate..
<SPAX> =/
<XsickboyX> ogni volta che voglio indicare quel gruppo
<XsickboyX> ricorda che sto facendo una lezione in chat
<XsickboyX> e nn è semplice
<Ripper> •4,15 non ci sono altre domande direi di continuare
<SPAX> non voglio confonderti o rallentarti scusami
<XsickboyX> no figurati
<SPAX> solo che se scrivi root è la gente che si confonde
<XsickboyX> ma datemi una mano anche voi
<XsickboyX> ok

<XsickboyX> ALLORA
<XsickboyX> X ADMIN INTENDO IL GRUPPO ADMINISTRATORS PRESENTE SU SISTEMI WIN NT
<Ripper> :)
<XsickboyX> E PER "PRIVILEGI ROOT" INTENDO I PRIVILEGI CHE UN UTENTE PUò
USUFRUIRE
<XsickboyX> CIOè PARDON
<XsickboyX> "privilegi di root o privilegio root " LO USO X INDICARE UN ACCOUNT
CON PRIVILEGI DI AMMINISTRATORE
<XsickboyX> CIOè CHE SI TROVA NEL GRUPPO ADMINISTRATORS
<XsickboyX> mi scuso x la distrazione
<XsickboyX> ok continuiamo
<XsickboyX> descriviamo ste 4 tecniche x ottenere il sam
<XsickboyX> TECNICA 1: ESEGUIRE UN BOOT
<XsickboyX> generalmente
<XsickboyX> questa tecnica è usata, come è ovvio, solo se avete accesso fisico
al pc
<XsickboyX> cioè se stase a scuola
<XsickboyX> nn ci vuole nulla prepararsi
<XsickboyX> un disco di boot da casa
<XsickboyX> e fare il boot diverso
<XsickboyX> e magari copiarlo su un altro floppy disk
<XsickboyX> visto che il SAM in genere è un file piccolo
<XsickboyX> basta prepararsi un disco di boot x dos con la utility COPY
<XsickboyX> (LA RICORDATE)
<XsickboyX> se nn erro
<XsickboyX> la grammatica è questa
<XsickboyX> copy percorso del file da copiare (es
c:\systemroot\System32\config\SAM) directory su cui copiare (es. A:\)
<XsickboyX> ok?
<XsickboyX> se
<Sbirilindo> aspetta
<Sbirilindo> sick
<XsickboyX> il sistema NT
<XsickboyX> dimmi
<XsickboyX> sbiri
<Sbirilindo> quindi il comando completo è?
<XsickboyX> c:\> copy c:\WinNT\System32\config\SAM a:\
<Sbirilindo> fammi un esempio
<Sbirilindo> ok
<XsickboyX> questo
<XsickboyX> questo comando può essere fatto DOPO UN RIAVVIO DA BOOT!!!
<XsickboyX> se lo fate con winnt in esecuzione, non andrà mai
<XsickboyX> ok?
<XsickboyX> dicevo...
<XsickboyX> se nel sistema operativo ci sono partizioni formattate con file
sistem NTFS
<XsickboyX> x accedere al disco abbiamo bisogno caricare un driver di sistema
l'NTFSDOS
<XsickboyX> lo trovate su http:\www.sysinternals.com
<XsickboyX> ok
<XsickboyX> dimmi
<XsickboyX> ok
<XsickboyX> il suddetto NTFSDOS
<XsickboyX> permette di usare le unità NTFS
<XsickboyX> come se fossero FAT32
<XsickboyX> ok?
<XsickboyX> se nn abbiamo la possibilità di fare un boot come si fa???
<XsickboyX> TECNICA n°2: uso della copia di backup della dir repair
<XsickboyX> che cos'è?
<XsickboyX> allora
<XsickboyX> ogni volta che viene avviamo l'utility rdisk (repair disk utility)
<XsickboyX> utilizzando il paramentro /s
<XsickboyX> che consente di fare copie di sicurezza
<XsickboyX> delle informazioni di configurazione
<XsickboyX> X GLI OP
<XsickboyX> LA PROSSIMA LEZIONE LUNEDI PROX
<XsickboyX> thx alex
<XsickboyX> dicevamo

<XsickboyX> utilizzando rdisk
<XsickboyX> con il paramentro /s
<XsickboyX> cioè c:\> rdisk /s
<XsickboyX> si crea un file SAM._
<XsickboyX> nella dir systemroot\repair
<XsickboyX> che non è affatto protetta!!!
<XsickboyX> la maggior parte degli admin (AMMISTRATORI)
<XsickboyX> non si preoccupa a pulire questa directory
<XsickboyX> quindi :)
<XsickboyX> allora
<XsickboyX> una volta bekkato sto file SAM._
<XsickboyX> lo dovete decomprimere
<XsickboyX> se usate LophtCrack questa funzione avviene automaticamente
<XsickboyX> ok
<XsickboyX> se
<XsickboyX> invece volete dare il sam
<XsickboyX> ad altri bruceforcer
<XsickboyX> dovete usare il programma
<XsickboyX> expand di windows
<XsickboyX> con la seguente grammatica
<XsickboyX> c:\> expand sam._ sam
<XsickboyX> x quanto riguarda lophtcrack
<XsickboyX> basta usare o il wizard
<XsickboyX> (cioè la procedura guidata :)
<XsickboyX> o il comando import file sam
<XsickboyX> e lui scompatterà il SAM
<XsickboyX> automaticament e vi darà gli users
<XsickboyX> le pass le dovete crakkare
<XsickboyX> e LC è ottimo
<XsickboyX> insomma x farvi capire
<XsickboyX> PRIMA O POI LA BEKKARE LA PASS!
<XsickboyX> DOMANDE!
<geek> lol
<zioponch> allora sick una volta preparato il floppy con il boot coma faccio il riavvio?e il fatto che lo creo da casa e faccio il boot diverso copiando su un altro floppy?
<zioponch> come faccio?
<XsickboyX> allora
<XsickboyX> pionche semplice
<Ripper> ma i floppy di boot vanno bene tutti...
<XsickboyX> il boot lo fai da casa e come dice giustamente ripper
<XsickboyX> vanno bene tutti
<XsickboyX> COME FAI A FARE UN BOOT?????
<XsickboyX> AHIAHIAHAIHA
<XsickboyX> basta inserire il disketto
<XsickboyX> nel floppy disk del pc
<XsickboyX> e premere il pulsante reset o riavviare normalmente il opc
<zioponch> quindi basta che metto i file system che fanno da boot?
<Ripper> zioponch spiegati meglio
<XsickboyX> ?
<XsickboyX> basta che crei un disko di avviamento
<XsickboyX> e lo inserisci nel sistema vittima
<zioponch> ok
<Ripper> crei un disco di avvio - resetti il pc - copi il file sam
<zioponch> ma winxp lo fa lo stesso?
<Ripper> si tutti i sistemi sono uguali
<Ripper> altro utente
<Ripper> vai somebody
<somebody> allora
<somebody> <XsickboyX> il suddetto NTFSDOS
<somebody> <XsickboyX> permette di usare le unità NTFS
<somebody> <XsickboyX> come se fossero FAT32
<XsickboyX> si zio ponch
<XsickboyX> dimmi
<somebody> senza ntfsdos invece
<somebody> come farei?
<XsickboyX> non lo so
<XsickboyX> io uso quel boot

<XsickboyX> e funzionaù
<XsickboyX> nn conosco altre
<XsickboyX> tecniche
<XsickboyX> anzi se ne sai qualcuna tu
<XsickboyX> diccela
<XsickboyX> che ampliamo l'argomento
<somebody> no non so
<XsickboyX> SIA CHIARO!!! ANCHE SE LE CHIAMIAMO LEZIONI IO NON SONO UN MAESTRO QUINDI
<XsickboyX> QUANDO PARLO DI UN ARGOMENTO E VOLETE AGGIUNGERE QUALCOSA SIETE I BENVENUTI!!!!
<XsickboyX> FATE CRESCERE ME E GLI ALTRI
<Ripper> --- procediamo non ci sono altre domande ----
<XsickboyX> ALLORA
<XsickboyX> VOLEVO DIRE STA COSA
<XsickboyX> OVViAMENTE
<XsickboyX> nonostante stia da tanto tempo in rete
<XsickboyX> NON
<XsickboyX> posso conoscere tutto di tutti i sistemi operativi
<XsickboyX> e, come penso che giusto sia, condivido le mie conoscenze
<XsickboyX> quindi rinnovo l'invito
<XsickboyX> chiunque conosca una tecnica INERENTE a quella di cui sto parlando io
<XsickboyX> me la dice in pvt
<XsickboyX> OK?
<XsickboyX> GRAZIE
<XsickboyX> le tecniche che mancano
<XsickboyX> è la cattura delle hash delle pass
<XsickboyX> senza bekkare
<XsickboyX> il SAM
<XsickboyX> e lo sniffing
<XsickboyX> quest'ultimo lo spiegabvo
<XsickboyX> spiegherò
<XsickboyX> quando parleremo del man in the middle
<XsickboyX> l'estrazione diretta la trattiamo adesso
<XsickboyX> allora
<XsickboyX> x questa tecnica
<XsickboyX> abbiamo bisogno
<XsickboyX> di un account con privilegi di admin
<XsickboyX> la tecnica consiste
<XsickboyX> nel prelevale le hash delle pass (cioè le pass criptate)
<XsickboyX> direttamente dal registro di configurazione di sistema
<XsickboyX> il programma in grado di far questo è pwdump
<XsickboyX> purtroppo su internet nn ho trovato un sito
<XsickboyX> ma in compenso
<XsickboyX> ho trovato un sito
<XsickboyX> che ha il file pwdump2
<XsickboyX> che aggira le protezioni SYSKEY
<XsickboyX> di cui parleremo tra un attimo
<XsickboyX> http://websapn.net/~tas/pwdump2/
<XsickboyX> x fare il carattere ~ chiamato tilde
<XsickboyX> basta tenere premuto l'alt di sinistra
<XsickboyX> e digitare 126 sul tastierino numerico
<XsickboyX> :)
<XsickboyX> Cmq LophtCrack ha anche questa funzione
<XsickboyX> quindi se avete le autorizzazioni di admin su un sistema
<XsickboyX> usate Lophtcrack
<XsickboyX> cmq
<XsickboyX> dicevamo
<XsickboyX> con il service pack 2
<XsickboyX> si è migliorato la cifratura del file sam e del registro di config
<XsickboyX> quindi useremo PWDUMP2
<XsickboyX> questa applicazione utilizza
<XsickboyX> il cosiddetto DLL injection
<XsickboyX> per poter caricare
<XsickboyX> un codice eseguibile
<XsickboyX> nello spazio di memoria
<XsickboyX> di un altro processo

<XsickboyX> che ha magari
<XsickboyX> maggiori privilegi
<XsickboyX> x far partire pwdump2
<XsickboyX> dobbiamo caricare il file avviabile e la libreria samdump.dll
<XsickboyX> sul sistema attakkato
<XsickboyX> e cmq avere l'account dell'amministratore
<XsickboyX> x la cronaca
<XsickboyX> il processo attakkato
<XsickboyX> da pwdump2
<XsickboyX> è lsass.exe
<XsickboyX> (Local Security Autorithy SubSistem)
<XsickboyX> il programma inserisce
<XsickboyX> (PWDUMP2) inserisce il proprio codice nello spazio di indirizzamento di lsass
<XsickboyX> per cui è necessario comunicare a pwdump2 il PROCESS ID (PID) di questo processo
<XsickboyX> la versione più recente di pwdump2
<XsickboyX> fa sta cosa automaticamente ma la accenno
<XsickboyX> c:\>pulist | find "lsass"
<XsickboyX> questo è quello che dobbiamo scrivere in remoto
<XsickboyX> x avere il PID di lsass
<XsickboyX> vi esce una cosa del genere
<XsickboyX> lsass.exe 50 NT AUTORITHY\SYSTEM
<XsickboyX> il pid di lsass quindi è 50
<XsickboyX> pwdump2
<XsickboyX> è usato con questa grammatica
<XsickboyX> c:\>pwdump2 50 (cioè il PID)
<XsickboyX> e vi escono tutti
<XsickboyX> tutte le hash
<XsickboyX> è stato un paicere
<XsickboyX> e vi ringrazio dell'attenzione
<XsickboyX> se avete domande
<XsickboyX> fatene adesso
<XsickboyX> :)
<Ripper> sick hai spiegato 3 tecniche vero ?
<XsickboyX> sonosi
<somebody> <XsickboyX> pwdump2
<somebody> <XsickboyX> è usato con questa grammatica
<somebody> ah no scusa
<XsickboyX> la quarta la spiego quando spiego la tecnica del MAN IN THE MIDDLE
<somebody> ho sbagliato
<somebody> aspetta
<Ripper> ok
<XsickboyX> fai fai
<somebody> vabbe
<somebody> comunque
<somebody> hai detto
<XsickboyX> zio ponch domande???? :)
<somebody> che da administrator
<somebody> si usa l0phtcrack
<somebody> ma se sono admin ke cracko a fare??
<XsickboyX> somebody
<zioponch> sick
<XsickboyX> se come dissi la scorsa volta
<zioponch> x me
<Sbirilindo> ciao raga
<zioponch> è tutto chiaro
<XsickboyX> è preferibile NON usate l'account admin
<XsickboyX> sempre
<XsickboyX> in quanto i log
<XsickboyX> "parlano"
<Sbirilindo> ci vediamo
<XsickboyX> bekkando il SAM
<zioponch> solo che x tirarmi fuori i dubbi dovrei provare e nn mi è tanto possibile
<XsickboyX> hai praticamente TUTTI gli user con relative PASSWORD
<XsickboyX> del sistema
<somebody> be ma che me ne faccio dell'account

<somebody> di un normale user
<somebody> ?
<XsickboyX> beh pensa se il pc
<XsickboyX> è una "porta d'accesso" ad un sistema
<XsickboyX> di rete
<Sbirilindo> grazie
<XsickboyX> più complesso
<XsickboyX> e solo alcuni account
<XsickboyX> possono accedere agli altri sistemi
<XsickboyX> :)
<somebody> poi volevo solo farti notare
<somebody> che
<XsickboyX> sia kiaro io spiego tutte le tecniche
<XsickboyX> sta a voi scegliere quale usare a seconda delle vostre esigenze
<somebody> si dice bruteforce e non bruceforce
<XsickboyX> dimmi
<somebody> come
<XsickboyX> errore di digitazione
<somebody> hai detto due volte
<XsickboyX> pardon
<XsickboyX> :)
<somebody> ah
<XsickboyX> somebody
<XsickboyX> prova a contare quante parole
<XsickboyX> ho scritto
<XsickboyX> ;)
<k3y> .
<somebody> eheh
<XsickboyX> ci saranno migliaia di errori di grammatica
<XsickboyX> ma nn ci bado tanto
<zioponch> ma importa il succo
<XsickboyX> :)
<XsickboyX> appunto
<XsickboyX> altro?
<XsickboyX> ok... vi ringrazio x la vostra attenzione :)
<XsickboyX> a lunedi
Session Close: Tue Oct 28 23:20:59 2003