Session Start: Thu Oct 02 21:10:56 2003
Session Ident: #AlexMessoMalex
* Now talking in #AlexMessoMalex
* Topic is '•11,2•www.AlexMessoMalex.com•• •8,2Stasera alle ore 22:00 CHAT MEETING• •4,0I LOG di ieri sono sul sito!!!••'
* Set by AlexMessoMalex_away on Thu Oct 02 17:36:31

<SaNdStOrM> quando arriva sickboy iniziamo
<SaNdStOrM> al massimo rimandiamo
<SaNdStOrM> adesso vediamo
<SaNdStOrM> se qualcuno riesce a sapere qualcosa
<AlexMessoMAlex> a qualcuno interessa un breve ripasso su TelNet mentre aspettiamo?
<darkernel> si si
* AlexMessoMAlex sets mode: +m
<AlexMessoMAlex> Ragazzi forse interessa a pochi ma intanto non abbiamo niente da fare...
<AlexMessoMAlex> Faccio un breve ripassino sull'invio di Fake Mail con Telnet
<AlexMessoMAlex> visto che un sacco di gente mi chiede come fare
<AlexMessoMAlex> e il 90% delle volte le persone non riescono per delle stupidate
<AlexMessoMAlex> Probabilmente è colpa anche della guida di Lord Shinva che non è molto chiara
<AlexMessoMAlex> però in questo modo tutte le e-mail che ci inviano potremo dirigerle sui log di questo meeting :)
<AlexMessoMAlex> Allora la cosa che sbagliano in tantissimi è l'SMTP Server
<AlexMessoMAlex> Quasi tutti sanno che i provider per farsi concorrenza vietano agli IP degli altri provider
<AlexMessoMAlex> di inviare e-mail tramite i loro server di posta in uscita
<AlexMessoMAlex> Perciò o trovate un server SMTP che permette l'invio di e-mail da qualsiasi IP oppure dovete utilizzare quello del vostro provider
* XSickBoyX has joined #alexmessomalex
<AlexMessoMAlex> cioè quello con cui siete collegati in quel momento
<baSheR> AlexMessoMAlex ora continua
<AlexMessoMAlex> Se ad esempio avete un contratto ADSL con Libero o vi collegate con il modem ad un pop d'accesso di Libero dovete utilizzare il server SMTP di Libero
<baSheR> mi sa che e meglio dei ping :P
<XSickBoyX> eccomi ragazzi
<AlexMessoMAlex> cioè mail.libero.it
<XSickBoyX> scusate il ritardo ma ho fatto tardi dal lavoro
<XSickBoyX> prego
<AlexMessoMAlex> Ovviamente dovete collegarvi alla porta 25 (quella che offre il servizio SMTP)
<AlexMessoMAlex> Non è necessario che scarichiate un TelNet, se usate Windows potete utilizzare benissimo quello
<AlexMessoMAlex> Cioè Avvio - Esegui - Telnet - OK (semplicissimo no?)
<AlexMessoMAlex> ad esempio con Win2000 appena avviato TelNet per collegarvi utilizzate il comando
<AlexMessoMAlex> open mail.libero.it 25
<AlexMessoMAlex> una volta connessi il server di Libero vi risponderà
<AlexMessoMAlex> 220 smtp2.libero.it ESMTP Service (7.0.020-DD01) ready
<AlexMessoMAlex> o qualcosa del genere
<AlexMessoMAlex> il primo comando è questo per "salutare" il server :)))
<AlexMessoMAlex> helo esempio.it
<AlexMessoMAlex> poi il mittente :
<AlexMessoMAlex> mail from: <mittente@mittente.it>
<AlexMessoMAlex> poi il destinatario :
<AlexMessoMAlex> rcpt to: <destinatario@destinatario.it>
<AlexMessoMAlex> poi il corpo del messaggio iniziate con il comando
<AlexMessoMAlex> data
<AlexMessoMAlex> mettete un po' di header dell'e-mail, ad esempio :
<AlexMessoMAlex> Received: by esempio.it id AA15684 with SMTP; Sun, 05 Oct 03 13:40:58
<AlexMessoMAlex> From: mittente@mittente.it
<AlexMessoMAlex> To: destinatario@destinatario.it

<AlexMessoMAlex> Date: Sun, 05 Oct 03 18:30:27
<AlexMessoMAlex> Subject: questo e' il titolo
<AlexMessoMAlex> gli header sono importanti altrimenti il provider si accorge che l'e-mail non è valida
<AlexMessoMAlex> poi scrivete il testo del messaggio
<AlexMessoMAlex> e quando avete finito scrivete un punto e premete INVIO
<AlexMessoMAlex> infine con il comando quit l'e-mail verrà inviata
<AlexMessoMAlex> scusate se sono stato troppo sintetico
<AlexMessoMAlex> ma siamo in ritardo :)

RIEPILOGO :

Dopo esservi collegati alla porta 25 del server SMTP del vostro provider :

helo esempio.it
mail from: <mittente@mittente.it>
rcpt to: <destinatario@destinatario.it>
data
Received: by esempio.it id AA15684 with SMTP; Sun, 05 Oct 03 13:40:58
From: mittente@mittente.it
To: destinatario@destinatario.it
Date: Sun, 05 Oct 03 18:30:27
Subject: questo e' il titolo

questo e' il messaggio
.
quit

<AlexMessoMAlex> Ovviamente destinatario@destinatario.it deve essere un indirizzo esistente, fate una prova su voi stessi con un vostro indirizzo (anche come mittente inserite un vostro indirizzo così nel caso qualcosa non vada il provider vi tornerà indietro l'e-mail specificando motivo)

<SaNdStOrM> ok iniziamo ora
<AlexMessoMAlex> domande?
<Rasta`][v][an> no tutto chiaro =o9
<darkernel> tutto kiaro;)
<AlexMessoMAlex> ah, l'ultima cosa
<XSickBoyX> Bene.....
<HolySniper> dai sick
<AlexMessoMAlex> se volete visualizzare le cose che digitate
<AlexMessoMAlex> sempre da TelNet prima di collegarvi
<AlexMessoMAlex> digitate: set local_echo
<AlexMessoMAlex> ;)
<ilfalco> alex
<TommyX> ?
<TommyX> ??
<TommyX> ???
<ilfalco> mi hai lasciato nel pvt
<m4rdXx> emh...vorrei salutare tutto in chan
<m4rdXx> è stato un piacere
<m4rdXx> ave a tutti :)
<ilfalco> puoi tornare un minuto
<XSickBoyX> Ciao m4rdxx
<TommyX> AlexMessoMalex: io vedo quello che digito in telnet...tranne le password ovviamente
<AlexMessoMAlex> bene
<TommyX> senza fare quello stupido comando
<XSickBoyX> dipende
<XSickBoyX> dalle versioni telnet
<XSickBoyX> di solito
<XSickBoyX> i comandi telnet
<XSickBoyX> nn si vedono
<XSickBoyX> e cmq
<TommyX> uso quella di win 98
<XSickBoyX> quando sbagliate
<XSickBoyX> un carattere
<XSickBoyX> rifate tutto d'accapo

<XSickBoyX> non usate in backspace
<AlexMessoMAlex> TommyX va bene lo stesso
<Prometeo> HyperTerminal?
<Rasta`][v][an> ovvio ;D
<XSickBoyX> xkè anche se sembra funzionare
<_david_> allora sick s parte??
<XSickBoyX> nn sempre va
<XSickBoyX> ok
<XSickBoyX> posso moderare????
<darkernel> inziamo:D
<baSheR> usate putty :)
<darkernel> :))))))))))
<baSheR> e buono
<dark87> salve
* SaNdStOrM si può iniziare ora
* XSickBoyX sets mode: +m
<XSickBoyX> ok
<XSickBoyX> ecco fatto
<XSickBoyX> innanzitutto
<XSickBoyX> buonasega a tutti
<XSickBoyX> ;)
<XSickBoyX> e scusate il ritardo
<XSickBoyX> ma lavoro
<XSickBoyX> allora
<XSickBoyX> partiamo subito
<XSickBoyX> senza perdere tempo
<XSickBoyX> allora
<XSickBoyX> ieri parlammo di whois
<XSickBoyX> e traceroute
<XSickBoyX> spero sono stato chiaro
<XSickBoyX> cmq trovate
<XSickBoyX> tutto su www.alexmessomalex.com nella sezione guide/chat
<XSickBoyX> nel senso che trovate il log
<XSickBoyX> della prima chattata
<XSickBoyX> quindi chi l'ha persa va lì
<XSickBoyX> oggi parliamo di ping
<XSickBoyX> e di scan...
<XSickBoyX> beh voi dire
<XSickBoyX> direte
<XSickBoyX> che cazzo c'è da dire sul ping???
<XSickBoyX> e invece c'è!!!!!!!!
<XSickBoyX> ed ecco cosa
<XSickBoyX> ogni bwel winzozz ha il suo ping.exe
<XSickBoyX> a cosa serve??
<XSickBoyX> il pin (la grammatica è questa : ping ippcvittima
<XSickBoyX> es ping 125.125.124.1)
<XSickBoyX> noi mandiamo
<XSickBoyX> un pakketto
<XSickBoyX> al pc vittima
<XSickBoyX> e lui ci risponde
<XSickBoyX> a che scopo??
<XSickBoyX> semplicemente x vedere se il pc vittima
<XSickBoyX> è opresente
<XSickBoyX> e a noi a cosa serve il ping????
<XSickBoyX> a questo....
<XSickBoyX> innanzitutto
<XSickBoyX> serve a vedere appunto i computer "up"
<XSickBoyX> x linux
<XSickBoyX> consiglio fping
<XSickBoyX> che ha tante funzioni
<XSickBoyX> o NMAP
<XSickBoyX> uscito pure x winzozz
<XSickBoyX> parliamo di nmap
<XSickBoyX> grande programma tuttofare
<XSickBoyX> facciamo il caso che abbiamo il nostro bel linus
<XSickBoyX> proviamo a digitare
<XSickBoyX> [bash] nmap -sP 192.168.125.0/24
<XSickBoyX> cosa è sp????

<XSickBoyX> è un ping sweep
<XSickBoyX> cosa vuol dire????
<XSickBoyX> nada in particolare alla fine
<XSickBoyX> visto che nmap supporta tante funzioni
<XSickBoyX> l'opzione x attivare il pin è -sP
<XSickBoyX> altre opzioni (che io conosco :))
<XSickBoyX> sono -d x risolvere i nomi host
<XSickBoyX> -f per scrivere l'output in un file
<XSickBoyX> cmq basta digitare -h e vi dà tutte le opzioni
<XSickBoyX> cmq le più usate sono queste
<XSickBoyX> torniamo all'esempio di prima
<XSickBoyX> che cos'è quell ip strano??? 192.168.125.0/24?
<XSickBoyX> abbiamo semplicemente detto a nmap di fare un ping di tutti gli ip che hanno come num finale da 0 a 24
<XSickBoyX> il nostro caro nmap
<XSickBoyX> ci dirà tutti gli host "up"
<XSickBoyX> cio+ connessi e funzionanti
<XSickBoyX> (alcuni pc possono essere anche in stato di freeze cioè connessi ma inattivi)
<XSickBoyX> Altri pinger conosciuti sono
<XSickBoyX> appunto pinger di rhino9
<XSickBoyX> che è comodo ee ha un'interfaccia grafica abb funzionale
<XSickBoyX> adesso veniamo
<XSickBoyX> alla cosa interessante di nmap
<XSickBoyX> facciamo il caso che digito una cosa del genere
<XSickBoyX> nmap -sP -PT25 195.125.1.0/24
<XSickBoyX> il nostro caro nmap
<XSickBoyX> farà il nostro bel ping
<XSickBoyX> (sono ping icmp
<XSickBoyX> poi vedremo se un firewall ferma gli ICMP come possiamo passarlo)
<XSickBoyX> A TUTTI i sistemi SOLO ALLA PORTA 25!!!!
<XSickBoyX> cosa ci serve sapere
<XSickBoyX> quale porta è aperta???
<XSickBoyX> beh una porta corrisponde ad un servizio
<XSickBoyX> e un servizio (tipo l'smtp) può avere bug
<XSickBoyX> :)
<XSickBoyX> andiamo avanti
<XSickBoyX> visto che abbiamo parlato di scan di porte (che poi è la cosa più interessante del ping
<XSickBoyX> andiamo ad approfondire st'argomento
<XSickBoyX> aspe
<XSickBoyX> forse è meglio vedere se ci sono domande
<XSickBoyX> chi ha domande
<XSickBoyX> query
<XSickBoyX> o a me o ad alex o a sand
* XSickBoyX sets mode: -m
<XSickBoyX> domande?
<KillA^^> a che serve pingare un ip? :D
<XSickBoyX> x vedere se attivo
<Prometeo> com'è possibile pingare una porta e non un host?
<XSickBoyX> a noi in particolare
<XSickBoyX> serve pingare una porta x vedere se una certa porta è attiva
<XSickBoyX> prometeo
<XSickBoyX> tu pingi la porta di un host
<baSheR> ihih
<Prometeo> Ma allora non è un vero PING
<XSickBoyX> posso andare avanti???
<baSheR> AlexMessoMAlex ..... :)
<XSickBoyX> come non è un vero ping
<Prometeo> sarà tuttalpiù un tentativo di connessione su quella porta, no?
<XSickBoyX> POSSONO PARLARE TUTTI
<XSickBoyX> no
<_david_> + o meno
<XSickBoyX> è un invio di pacchetti ICMP
<fantoibed> 1) Che c'azzeccano le porte con i ping?
<fantoibed> i ping sono pacchetti icmp
<darkernel> SEKONDO ME E SEMPRE UN INVIO DI PAKKETTI E RICEVI DELLE RISPOSTE E' SEMPRE UN PING

<baSheR> tentativo di connessione manda un syn poi lo tratteranno credo :P
<fantoibed> che non hanno porte
<XSickBoyX> dove il nostro host bersaglio rispondera con un ICMP echo reply
<XSickBoyX> il syn è n'altra cosa
<XSickBoyX> fanto
<baSheR> si appunto dicevo a Prometeo
<XSickBoyX> i PING SONO SOLO PAKKETTI DI DATI
<fantoibed> echo reply è uno dei 15 sottotipi, non una porta... :-)
<Prometeo> fantoibed: hai capito cosa m'intendo
<XSickBoyX> CHE TU MANDI ALLE PORTE DI UN HOST
<XSickBoyX> UN HOST è UN PC
<XSickBoyX> OK?
<Master^Shadow> -PT   Use TCP "ping" to determine what hosts are up. Instead of send-
<Master^Shadow>   ing ICMP echo request packets and waiting for a response, we
<Master^Shadow>   spew out TCP ACK packets throughout the target network (or to a
<Master^Shadow>   single machine) and then wait for responses to trickle back.
<fantoibed> 2) il /24 dell'indirizzo che hai riportato
<fantoibed> non significa quello che dici tu
<fantoibed> è il numero di bit della netmask
<XSickBoyX> si pardon
<Prometeo> fantoibed: abbiamo le stesse idee
<paolo23> sera
<XSickBoyX> li errore mio
<XSickBoyX> sto dando
<XSickBoyX> un'okkiata a nmap
* XSickBoyX sets mode: +m
<XSickBoyX> allora
<XSickBoyX> Pardon
<XSickBoyX> sono un incompetente
<XSickBoyX> :))
<XSickBoyX> fantoibed
<XSickBoyX> mi ha fatto notare una cosa
<XSickBoyX> quando mettete l'ip 125.125.125.1/24
<XSickBoyX> il /24
<XSickBoyX> non è il range
<XSickBoyX> di
<XSickBoyX> ip
<XSickBoyX> ma il range di ip si fa col trattino
<XSickBoyX> pardon
* XSickBoyX sets mode: -m
<XSickBoyX> rieccovi la voce
<XSickBoyX> altre domande??
<Prometeo> si
<XSickBoyX> dimmi
<Prometeo> ascolta io non ho capito cosa centra un ping con le porte
<XSickBoyX> prometeo
<XSickBoyX> mai usato subseven=???
<XSickBoyX> detto pratico
<XSickBoyX> tu x vedere
<XSickBoyX> se un pc
<AnToNiN> we ragaa
<Prometeo> se io mando un ping sulla porta 25 a rispondermi sarà il servizio SMTP e non l'ICMP
<XSickBoyX> ha una porta
<fantoibed> è da lamerozzi il sub7
<fantoibed> :-)
<XSickBoyX> si era come esempio :)))
<AnToNiN> mi dite kome rikavare un ip di una persona ke chatta kn me in C6?
<XSickBoyX> il ping NON è una connessione
<XSickBoyX> antonin
<XSickBoyX> non adesso
<fantoibed> Prometeo: l'icmp è un formato non un servizio
<Prometeo> scusa scusa
<AnToNiN> :(((e quando?

<Rasta`][v][an> mi dite come criptare un v6?
<fantoibed> sono a 2 diversi livelli della pila iso/osi
* XSickBoyX sets mode: +m
<XSickBoyX> aspettate raga
<XSickBoyX> si sta facendo un bordello
<XSickBoyX> allora
<XSickBoyX> PRIMA COSA
<XSickBoyX> CAZZO SIA CHIARO
<XSickBoyX> IO NON SPAMMO NEGLI ALTRI CANALI
<XSickBoyX> SIA CHIARO
<XSickBoyX> PRIMA DI FARE PUBBLICITà A QUESTO CORSO
<XSickBoyX> SU ALTRI CHAN
<XSickBoyX> O ERANO I MIEI
<XSickBoyX> O CMQ HO CHIESTO L'AUTORIZZAZIONE ALL'ADMIN
<XSickBoyX> detto questo
<XSickBoyX> antonin non chiedere
<XSickBoyX> come si cerca un ip da c6 NON QUI!
<XSickBoyX> allora
* AlexMessoMAlex sets mode: -m
<l0rdr0x> we Zorro
<Kupo`> atò quante pesone
<Kupo`> °_°_°_°_°
<XSickBoyX> allora
<XSickBoyX> continuo
* XSickBoyX sets mode: +m
<XSickBoyX> allora brevemente
<XSickBoyX> il ping
<XSickBoyX> viene utilizzato
<XSickBoyX> x inviare pakketti
<XSickBoyX> ICMP ECHO
<XSickBoyX> ad un sistema obiettivo
<XSickBoyX> e si sollecita la restituzione di un pacchetto di tipo ICMP ECHO_Reply
<XSickBoyX> che indica che il sist è in funzione
<XSickBoyX> ok?
* XSickBoyX sets mode: -m
<XSickBoyX> posso andare avanti?
<XSickBoyX> POSSONO PARLARE TUTTI
<darkernel> certo ke si
<active85k> beh credo di si
<darkernel> vai vai:))))
<paolo23> avanti avanti :)
* XSickBoyX sets mode: +m
<XSickBoyX> ok
<XSickBoyX> una volta
<XSickBoyX> visto
<XSickBoyX> che il nostro sistema obiettivo
<XSickBoyX> è attivo
<XSickBoyX> procediamo alla scansione
<XSickBoyX> delle porte in stato di listening su un sistema
<XSickBoyX> stato di listening vogliono dire aperte
<XSickBoyX> e pronte a ricevere una connessione
<XSickBoyX> ok
<XSickBoyX> ?
<XSickBoyX> allora facciamo degli scan
<XSickBoyX> a che scopo?
<XSickBoyX> fondamentalmente a tre
<XSickBoyX> 1 IDENTIFICAZIONE DEI SERVIZI TCP E UDP IN ESECUZIONE SUl nostro sistema obiettivo
<XSickBoyX> 2 identificazione del sistema operativo sul nostro sistema obiettivo
<XSickBoyX> 3 identificazione di particolari applicazioni
<XSickBoyX> Allora
<XSickBoyX> ci sono vari tipi di scan
<XSickBoyX> e vi dico i più famosi
<XSickBoyX> "conosciuti"
<XSickBoyX> il TCP CONNECT SCAN
<XSickBoyX> è un tipo di scansione che si collega al sistema obiettivo e che usa la procedura SYN, SYN/ACK, ACK

<XSickBoyX> questo scan viene facilmente identificato dal sistema obiettivo
<XSickBoyX> poi abbiamo il TCP SYN Scan
<XSickBoyX> è una scansione che non viene realizzata con una connessione TCP completa ma semi aperta
<XSickBoyX> il nostro pc manda il syn
<XSickBoyX> se il pc vittima risponde con syn/ack
<XSickBoyX> la porta è attiva
<XSickBoyX> se risponde con rst/ack la porta di solito è chiusa
<XSickBoyX> questa tecnica è decisamente più discreta
<XSickBoyX> Poi conosco
<XSickBoyX> il TCP Null Scan
<XSickBoyX> è una connessione nulla
<XSickBoyX> è molto discreta ma non sempre funziona
<XSickBoyX> Importante è la TCP ACK
<XSickBoyX> questa tecnica di solito viener usata per ricostruire
<XSickBoyX> la mappa dell'insieme
<XSickBoyX> di regole di un firewall
<XSickBoyX> in parole povere
<XSickBoyX> ci fa capire
<XSickBoyX> se un firewall che è attivo è un semplice filtro di pakketti
<XSickBoyX> o se il firewall
<XSickBoyX> ha attive funzionalità avanzate
<XSickBoyX> poi
<XSickBoyX> c'è l'udp scan
<XSickBoyX> x vedere i servizi
<XSickBoyX> UDP
<XSickBoyX> allora
<XSickBoyX> l'udp è un protocollo che non è basato sulla connessione
<XSickBoyX> quindi a volte può non andare
<XSickBoyX> e inoltre è estremamente lento
<XSickBoyX> allora
<XSickBoyX> adesso vediamo come si fanno sti tipi di scansioni
<XSickBoyX> allora
<XSickBoyX> c'è un progr sia x unix sia per winNT/2000
<XSickBoyX> si chiama strobe
<XSickBoyX> io mi trovo bene :)
<XSickBoyX> la grammatica
<XSickBoyX> è la seguente
<XSickBoyX> strobe ipvittima
<XSickBoyX> es strobe 125.24.58.1
<XSickBoyX> in nostro caro progr
<XSickBoyX> ci darà
<XSickBoyX> come risposta
<XSickBoyX> tutte le porte attive
<XSickBoyX> con relativo nominativo del servizio
<XSickBoyX> tipo
<XSickBoyX> 125.24.58.1 ftp 21/tcp File Tranfer [Control]
<XSickBoyX> quindi adesso sappiamo
<XSickBoyX> che l'ip
<XSickBoyX> 125.24.58.1
<XSickBoyX> ha la porta FTP in listening
<XSickBoyX> questo scan
<XSickBoyX> fa solo scanning TCP
<XSickBoyX> niente UDP :(((
<XSickBoyX> x gli udp
<XSickBoyX> posso citare udp_scan x linux
<XSickBoyX> grammatica semplice tipo
<XSickBoyX> udp_scan 125.25.25.1
<XSickBoyX> se volete specificare le porte
<XSickBoyX> udp_scan 125.25.25.1 1-10000
<XSickBoyX> Qui ci viene ancora in aiuto nmap
<XSickBoyX> come facciamo gli scan??
<XSickBoyX> brevemente
<XSickBoyX> allora
<XSickBoyX> -sT fa una connessione TCP
<XSickBoyX> -sU fa una connessione UDP
<XSickBoyX> -sP fa un ping scan (già detto prima)
<XSickBoyX> -O cerca di capire tramite scanning il sistema operativo della

makkina remota
<XSickBoyX> -p 1-10000
<XSickBoyX> indica le porte
<XSickBoyX> da scannare :)
<XSickBoyX> andiamo adesso con qualche esempio
<XSickBoyX> nmap -sT -p 1-10000 125.25.25.1
<XSickBoyX> ok??
<XSickBoyX> cmq
<XSickBoyX> le info su nmap
<XSickBoyX> come detto le trovate
<XSickBoyX> digitando
<XSickBoyX> nmap -h
<XSickBoyX> se avete windows
<XSickBoyX> come si fa?? (io ho provato la versione di nmap x win ma non mi va)
<XSickBoyX> ho fatto una breve ricerca
<XSickBoyX> e il migliorre è NetScanTools Pro
<XSickBoyX> che ha l'inverosimile di opzioni
<XSickBoyX> davvero tantte
<XSickBoyX> dai whois
<XSickBoyX> traceroute
<XSickBoyX> lookup
<XSickBoyX> ovviamente anche scanner
<XSickBoyX> tutto in interfaccia grafica
<XSickBoyX> quindi facile da capire
<XSickBoyX> nmap
<XSickBoyX> lo trovate su
<XSickBoyX> www.insecure.org/nmap
<XSickBoyX> l'altro su www.nwpsw.com
<XSickBoyX> mi pare che è a pagamento
<XSickBoyX> ma c'è una versione con meno opzioni ed è free
* XSickBoyX sets mode: -m
<XSickBoyX> POTETE PARLARE TUTTI
<XSickBoyX> domande?
<_david_> sick
<_david_> potresti mandarmi il log please?
<HolySniper> dai va avanti
<XSickBoyX> david
<HolySniper> david lo trovi sul sito domani
<XSickBoyX> lo trovi su alexmessomalex.com
<_david_> ah ok
<darkernel> meglio netmao o netscanner tools?
<_david_> c sendiamo
<XSickBoyX> posso andare avannti??
<darkernel> *netmap
<HolySniper> si sick
<XSickBoyX> nmap
<XSickBoyX> è ottimo
<HolySniper> dai avanti
<XSickBoyX> e veramente affidabile
<XSickBoyX> ok vado avanti
* XSickBoyX sets mode: +m
<XSickBoyX> adesso
<XSickBoyX> che abbiamo imparato lo scannig delle porte
<XSickBoyX> usiamolo oltre per sapere i servizi
<XSickBoyX> anche x sapere che OS gira sul pc vittima
<XSickBoyX> come saperlo???
<XSickBoyX> generalmente
<XSickBoyX> ci sono delle tecniche particolari
<XSickBoyX> le più famose sono
<XSickBoyX> una sonda FIN
<XSickBoyX> cioè un invio di un pakketto FIN su una porta aperta scelta come
obiettivop
<XSickBoyX> quando un pakketto fin
<XSickBoyX> viene ricevuto dfa una porta aperta
<XSickBoyX> il comportamento corretto sarebe non rispondere
<XSickBoyX> ma molte volte i WINNT rispondono con FIN/ACK
<XSickBoyX> ;)
<XSickBoyX> il valore ack

<XSickBoyX> cioè il valore di sequenza utilizzato
<XSickBoyX> x il campo ack
<XSickBoyX> varia a seconda dell'implementazione di ip
<XSickBoyX> in certi
<XSickBoyX> casi
<XSickBoyX> viene rrestituito
<XSickBoyX> con il num di sequenza avviato
<XSickBoyX> in altri è aumentato
<XSickBoyX> cmq quello chee sto dicendo è teoria
<XSickBoyX> dopo spiego come si fanno in pratica
<XSickBoyX> tranqui
<XSickBoyX> oppure
<XSickBoyX> possiamo capire
<XSickBoyX> un OS semplicemente
<XSickBoyX> dalle porte aperte
<XSickBoyX> se un OS avra la 134 o la 135 aperta
<XSickBoyX> è probabile che sia un win
<XSickBoyX> Nmap cmq supporta tutti questi tipi di scanning
<XSickBoyX> che possono aiutarci a farci capire
<XSickBoyX> che OOS è quello remoto
<XSickBoyX> prima abbiamo parlato
<XSickBoyX> della funzione -O di nmap
<XSickBoyX> adesso la utilizziamo
<XSickBoyX> facciamo il caso
<XSickBoyX> di usare nmap in questo modo
<XSickBoyX> nmap -o 125.25.25.1
<XSickBoyX> nmap farà uno scanning di questo sitema
<XSickBoyX> e alla fine
<XSickBoyX> ci dirà come output una cosa del genere
<XSickBoyX> remote operating system guess : Win NT o che ne so linux 2.0.27
<XSickBoyX> o quel che suia
<XSickBoyX> altra
<XSickBoyX> funzione
<XSickBoyX> no funzione pardon
<XSickBoyX> altra tecnica
<XSickBoyX> è una ricerca passiva
<XSickBoyX> che è fondamentalmente più discreta della prima
<XSickBoyX> che vuol dire?
<XSickBoyX> semplice
<XSickBoyX> al posto di inviare pakketti ect
<XSickBoyX> al sistema target
<XSickBoyX> ci limiteremo ad analizzare il suop traffico di rete
<XSickBoyX> fondamentalmente
<XSickBoyX> andiamo a studiare
<XSickBoyX> alcune proprietà del protocollo TCP/IP
<XSickBoyX> in particolare tre
<XSickBoyX> il TTL (ricordate? quello su cui si basa il traceroute)
<XSickBoyX> le dimensioni della finestra (non vi è mai capitato che un sito vi dice la vostra risoluzione e il tipo di browser che usate???)
<XSickBoyX> e il bit DF (don't fragment)
<XSickBoyX> allora come si fa tutto ciò???
<XSickBoyX> eseguiamo
<XSickBoyX> una sessione telnet
<XSickBoyX> quella di cui parlava alex prima
<XSickBoyX> verso
<XSickBoyX> il nostro
<XSickBoyX> sistema taerget
<XSickBoyX> telnet 125.25.25.1
<XSickBoyX> se utilizziamo uno sniffer
<XSickBoyX> tipo snort (ne parleremo nelle prossime lezioni)
<XSickBoyX> uscira una cosa del genere
<XSickBoyX> 124.251.142.1(il nostro IP) -> 1235.25
<XSickBoyX> cazzo
<XSickBoyX> 124.251.142.1:23 -> 125.25.25.1:2295
<XSickBoyX> tcp TTL:225 TOS:0x0 ID:58934 DF
<XSickBoyX> **S***A* SEQ: 0xD3B709A4
<XSickBoyX> (la prox lezione gli esempi me li faccio prima e poi copio e incollo)

<XSickBoyX> vabbe
<XSickBoyX> escono tanti numeretti
<XSickBoyX> a noi interessanno
<XSickBoyX> tre
<XSickBoyX> il TTL (time to live)
<XSickBoyX> il windowsd size (esce sotto la voce WIN)
<XSickBoyX> e il DF
<XSickBoyX> se c'è o meno
<XSickBoyX> cmq
<XSickBoyX> c'è un'applicazione comodissima
<XSickBoyX> x
<XSickBoyX> linux
<XSickBoyX> kiamata siphon
<XSickBoyX> la grammatica è questa
<XSickBoyX> siphon -v -i x10 -o temp.out
<XSickBoyX> fatto cio
<XSickBoyX> il nostro siphon avrà un output di questo tipo
<XSickBoyX> host 125.25.25.1
<XSickBoyX> ppotr 23
<XSickBoyX> ttl 255
<XSickBoyX> df on
<XSickBoyX> operating system SOLARIS 2.6 2.7
<XSickBoyX> perchè ciò?
<XSickBoyX> perchè a seconda di alcune caratteristice
<XSickBoyX> che
<XSickBoyX> siphon "sa"
<XSickBoyX> lui ci ridà il OS
* XSickBoyX sets mode: -m
* XSickBoyX sets mode: +m
<XSickBoyX> penso che x oggi vada bene così
<SaNdStOrM> si
<XSickBoyX> anche se ho lasciato tanto in disparte
<SaNdStOrM> la prossima lezione la faremo settimana prossima
<XSickBoyX> e mi rendo conto che ho fatto un casino della madona
<SaNdStOrM> domani sera e nel weekend mi sembra inutile visto che verrà poca gente
<XSickBoyX> la prox volta iniziamo prima mi scrivo una bella lezione con gli esempi e ve la incollo
<XSickBoyX> si
<XSickBoyX> martedi va bene???
* XSickBoyX sets mode: -m
<SaNdStOrM> ok
<XSickBoyX> DOMANDE????
<XSickBoyX> POSSONO PARLARE TUTTI
<baSheR> hiih sono svenuti =
<XSickBoyX> spero almeno di avervi fatto capire a che serve uno scan su un sistema
<baSheR> :/
<XSickBoyX> effettivamente
<XSickBoyX> è una palla
<paolo23> direi di si
<XSickBoyX> il prox argomento
<baSheR> lollllllll
<XSickBoyX> inziamo con l'hack di win NT
<baSheR> gh
<paolo23> domanda
<baSheR> cmq senti XSickBoyX che lavoro fai se si puo sapere eh =
<baSheR> ??
<paolo23> nn so se sia stato trattato in Ilezione
<XSickBoyX> prova paolo
<XSickBoyX> cazzop che mal di testa
<paolo23> quali tecniche si usano per far figurare al target un ip da noi voluto ?
<SaNdStOrM> a presto, buonanotte
<paolo23> ?
<paolo23> xsick
<XSickBoyX> si dimmi scusa
<XSickBoyX> mi stai chiedendo

<XSickBoyX> dell'ip Spoofing
<paolo23> quali tecniche si usano per far figurare al target un ip da noi voluto
?
<XSickBoyX> ne parleremo più in la
<XSickBoyX> ce ne sono tante di tecniche
<paolo23> ok
<paolo23> ma si deve usare prog apposta ?
<XSickBoyX> no
<paolo23> o in linux sono previsti comandi che fanno il servizio ?
<XSickBoyX> ma dobbiamo finire il discorso
<XSickBoyX> sullo scanning
<KoRnuto> ah
Session Close: Thu Oct 02 23:48:13 2003