Session Start: Wed Oct 01 20:52:42 2003
Session Ident: #AlexMessoMalex
* Now talking in #AlexMessoMalex
* Topic is '•11,2www.AlexMessoMalex.com• •0,12Per evitare ogni tipo di ripetizione, visitate il ••forum•• e la sezione ••FAQ•• prima di chiedere ai moderatori• •2,8Mercoledì •1° Ottobre• ore •21:00•: inizia il •CHAT-MEETING•••'
* Set by AlexMessoMalex on Wed Oct 01 15:37:23

<AlexMessoMalex> Ragazzi, prima di passare la parola a XSickBoyX volevo spendere 2 paroline
* XSickBoyX sets mode: -m
<XSickBoyX> un attimo
<XSickBoyX> ragazzi
<XSickBoyX> vi va bene se prima parliamo noi
<XSickBoyX> o almeno io
<XSickBoyX> e dopo domandate ciò che volete??
<AlexMessoMalex> infatti volevo dire questo :)
<SaNdStOrM> quello col + davanti tiene la lezione :-))
<AlexMessoMalex> se qualcuno non è d'accordo... fiiiuuuuuuuu :))
* SaNdStOrM sets mode: +m
<SaNdStOrM> inizia pure
<AlexMessoMalex> OK, adesso SickBoy farà la lezione senza interruzioni
<AlexMessoMalex> alla fine ci sarà tempo per le domande
<AlexMessoMalex> buon ascolto...
<SaNdStOrM> mi raccomando non queratelo
<XSickBoyX> allora raga
<XSickBoyX> iniziamo subito con una bella cosa
<SaNdStOrM> per chi fosse entrato solo ora, ripetiamo: ora parla sickboy, alla fine le domande
<XSickBoyX> Io, SickBoy, scrivo questa guida con lo scopo di divulgare le informazioni necessarie per proteggersi da attacchi esterni nel mondo della Rete. Mi astengo da ogni uso anomalo di terzi di questa guida.
<XSickBoyX> Tu, lettore, continuando a leggere questa guida, sollevi da ogni responsabilità SickBoy dell'uso che farai della seguente.
<XSickBoyX> sickb@email.it
<XSickBoyX> ;)
<XSickBoyX> un bel disclaimer
<XSickBoyX> allora parliamo subito della ricerca di informazioni su un server chee ci interessa
<XSickBoyX> ok?
<XSickBoyX> x farmi capire
<XSickBoyX> parlo di whois traceroute ect
<XSickBoyX> Allora
<XSickBoyX> parto a parlare
<XSickBoyX> velocemente in cosa consiste la ricerca di info su un determinato server
<XSickBoyX> allora
<XSickBoyX> iniziamo
<XSickBoyX> con ricerche a basso livello
<XSickBoyX> ci va bene pure su motori di ricerca
<XSickBoyX> possiamo bekkare
<XSickBoyX> tante belle cose
<XSickBoyX> tipo email
<XSickBoyX> di cambi di sicurezza
<XSickBoyX> acquisti di aziende
<XSickBoyX> grandi
<XSickBoyX> insomma tutte le info ci serviranno
<XSickBoyX> (anche se vogliamo fare un pò di ingegneria sociale
<XSickBoyX> andiamo sul pratico
<XSickBoyX> facciamo il caso
<XSickBoyX> che vogliamo attaccare
<XSickBoyX> il sito www.alexmessomalex.com
<XSickBoyX> :)))))))
<XSickBoyX> andiamo magari su altavista
<XSickBoyX> e possiamo fare una ricerca tipo link:www.alexmessomalex.com and hacking

<AlexMessoMalex> un sito a caso :)
<XSickBoyX> o and sicurezza
<XSickBoyX> o and la vostra fantasia
<XSickBoyX> magari troviamo qualcosa di interessante
<XSickBoyX> continuiamo
<XSickBoyX> facciamo il caso che la società obiettivo
<XSickBoyX> sia quotata pubblicamente
<XSickBoyX> possiamo fare riferimento al sito www.sec.gov
<XSickBoyX> insomma x ogni tipo di società c'è un luogo dove trovare info
<XSickBoyX> dopo la ricerca a mano libera
<XSickBoyX> andiamo a vedere la rete
<XSickBoyX> sarò breve xkè voglio trattare anche la ricerca in ambiente unixx
<XSickBoyX> ok?
<XSickBoyX> bene
<XSickBoyX> partiamo con i whois
<XSickBoyX> che sono delle query
<XSickBoyX> che facciamo a determintati server x bekkare info su un determinato host
<XSickBoyX> subito mi salta il nome di www.arin.net
<XSickBoyX> che ha un'interfaccia grafica
<XSickBoyX> o la stessa www.networksolutions.com
<XSickBoyX> x unix
<XSickBoyX> che il client whois incluso nella maggiorparte delle distro
<XSickBoyX> come se fanno i whois????
<XSickBoyX> allora dipende dal sito
<XSickBoyX> generalmente la cosa funziona così
<XSickBoyX> x gli Ip europei si usa il server whois.ripe.net
<XSickBoyX> x gli asiatici whois.apnic.net
<XSickBoyX> x i militari USA whois.nic.mil
<XSickBoyX> x i governativi USA nic.gov
<XSickBoyX> poi ci sono tanti server whois da poter usare quindi
<XSickBoyX> :)
<XSickBoyX> facciamo conto
<XSickBoyX> che abbiamo
<XSickBoyX> una linux
<XSickBoyX> ok?
<XSickBoyX> bene
<XSickBoyX> [bash] whois "nomesito."@whois.nomeserver.net
<XSickBoyX> generalmente funziona cosi
<XSickBoyX> il server ci darà una cosa tipo
<XSickBoyX> tutti i siti che contengono la parola nomesito
<XSickBoyX> da lì possiamo ricercare una cosa tipo
<XSickBoyX> whois "nomesito.it"@whois.nomeserver.it
<XSickBoyX> ed ecco le prime info reali
<XSickBoyX> l'output dovrebbe essere una
<XSickBoyX> cosa del genere
<XSickBoyX> Nome dominio: NOMESITO.net
<XSickBoyX> REGISTRAR: nomeregistrar
<XSickBoyX> server whois
<XSickBoyX> server whois : nome del server whois
<XSickBoyX> e i nome dei dns
<XSickBoyX> dei server dns
<XSickBoyX> da adesso in poi andremo ad usare com server whois il server del nostro sito
<XSickBoyX> tipo
<XSickBoyX> se il resistrar sarà network solutions
<XSickBoyX> andiamo su whois.networksolutions.cokm
<XSickBoyX> ok?
<XSickBoyX> altro database
<XSickBoyX> interessante
<XSickBoyX> è arin.net
<XSickBoyX> che ci dice chee grandezza ha un dominio
<XSickBoyX> facciamo il caso che il nostro obiettivo è pippo
<XSickBoyX> whois "pippo." @whois.arin.net
<XSickBoyX> da notare il punto dopo PIPPO
<XSickBoyX> il punto è il caro * in win
<XSickBoyX> cioè il carattere jolly :)
<XSickBoyX> beh dopo un migliaio di whois

<XSickBoyX> possiamo andare avanti
<XSickBoyX> (date libero sfogo alla vostra fantasia)
<XSickBoyX> rompiamo le scatole agli dns
<XSickBoyX> x win ci sono tantissimi progr
<XSickBoyX> che hanno tanti
<XSickBoyX> clieent
<XSickBoyX> whois
<XSickBoyX> ping
<XSickBoyX> scanner
<XSickBoyX> ect
<XSickBoyX> x unix
<XSickBoyX> ce ne sono altrettanti
<XSickBoyX> quindi nn avrete problemi
<XSickBoyX> adesso usiamo lo strumento nslookup
<XSickBoyX> che
<XSickBoyX> fa una cosa semplicissima ma essenziale
<XSickBoyX> facciamo il caso che pippo.com
<XSickBoyX> aspettate
<XSickBoyX> noi sappiamo
<XSickBoyX> che ogni computer
<XSickBoyX> è caratterizzato da un ip
<XSickBoyX> cioè
<XSickBoyX> un numero xxx.xxx.xxx.xxx
<XSickBoyX> tipo questo dove le x arrivano ad un max di 256
<XSickBoyX> allora
<XSickBoyX> se vogliamo sapere l'ip di pippo.com
<XSickBoyX> usiamo nslookup
<XSickBoyX> dicevamo
<XSickBoyX> nslookup è presente
<XSickBoyX> sia
<XSickBoyX> in unix sia in NT
<XSickBoyX> quindi avviamolo semplicemente
<XSickBoyX> poi gli scriviemo il nome del server
<XSickBoyX> e avremo l'ip
<XSickBoyX> adesso proviamo a fare un trasferimento di zona
<XSickBoyX> allora un trasf di zona
<XSickBoyX> consente
<XSickBoyX> ad un server master secondario
<XSickBoyX> di aggiornare il proprio database
<XSickBoyX> della zona rispetto ad un master primario
<XSickBoyX> cerchiamo di bekkarne l'output
<XSickBoyX> ok?
<XSickBoyX> avviamo nslookup
<XSickBoyX> e scriviamo server ipdns
<XSickBoyX> e poi digitiamo
<XSickBoyX> settype=any
<XSickBoyX> ls-pippo.com.>>/tmp/output
<XSickBoyX> se tutto cva bene
<XSickBoyX> dipende dalle impostazioni del server dns
<XSickBoyX> avremo info
<XSickBoyX> di alcuni pc
<XSickBoyX> e alcuni servizi
<XSickBoyX> presenti nella rete obiettivo
<XSickBoyX> ok
<XSickBoyX> prima pausa
<XSickBoyX> cari op
<XSickBoyX> attivate
<XSickBoyX> ;)
<XSickBoyX> sand
<XSickBoyX> leva la moderazione
<SaNdStOrM> ok
<XSickBoyX> una cosa
<SaNdStOrM> allora
<SaNdStOrM> si inizia con la prima parte di domande
<XSickBoyX> x favore NIENTE PING NIENTE SCAN sul mio pc ok?
<XSickBoyX> grazie
<SaNdStOrM> ora diamo il voice a 3 alla volta così possono parlare
<SaNdStOrM> affinchè tutti possano chiedere

<SaNdStOrM> iniziamo coi primi 3
<XSickBoyX> anche 5 alla volta
<XSickBoyX> altrimenti andiamo troppo piano
<SaNdStOrM> ok
<badboy84> nn ho niente da chiedere :-P passate pure ;-)
<SaNdStOrM> chi ha il + davanti può parlare
<Agareth> XSickBoyX: ma da linux il nslookup?
<darkernel>)))))
<XSickBoyX> sia da linux che da nt
<XSickBoyX> da console
<Agareth> io ho XP..
<SaNdStOrM> •0,2chi ha il + davanti può parlare
<Black^Jad> non ho niente da kiedere-potete passare
<darkernel> in teoria se uso il programma netlab
<darkernel> ke ha
<darkernel> whois
<darkernel> finger
<Freud> passo anch'io...aspetto altre informazioni
<XSickBoyX> si dark
<darkernel> non e' mejo e + semplice con quel programma
<XSickBoyX> basta un client lookup
<SaNdStOrM> •0,2chi ha il + davanti può parlare
<darkernel> ah ok
<Agareth> io ho XP..
<XSickBoyX> agareth
<HolySniper> una domanda su tutte, ho perso l'inizio, ci sono i log?
<SaNdStOrM> •0,12chi ha il + davanti può parlare
<XSickBoyX> ci sono vari tools anche x XP
<SaNdStOrM> si ci sono i log
<Agareth> quali? dove?
<XSickBoyX> cerca con motori di ricerca tools
<HolySniper> k thnx
<XSickBoyX> tipo genius 2
<XSickBoyX> o netlab
<HolySniper> allora, un'altra
<darkernel> esatto
<AlexMessoMalex> i log verranno pubblicati sul sito nei prossimi giorni
<AlexMessoMalex> bravi ragazzi, così si fa, ordinati e rispettosi, che bravi !
<Agareth> darkernel: mi sendi netlab?
<HolySniper> puoi spiegarmi cosa sono il server master secondario e primario?
<darkernel> basta ke cercki su google download netlab
<L0GAN> Ma tutti i server dns danno il risultato voluto?
<XSickBoyX> aspeeeeeee
<L0GAN> tutti quelli che hai elencato?
<XSickBoyX> uno alla volta
<XSickBoyX> allora
<XSickBoyX> ci sono sempre almeno due server dns
<XSickBoyX> uno master primario uno secondario
<XSickBoyX> LOGAN
<XSickBoyX> non tutti
<XSickBoyX> i master
<XSickBoyX> non tutti i server dns
<SaNdStOrM> •0,12chi ha il + davanti può parlare
<XSickBoyX> danno questo risultato
<XSickBoyX> DIpende dall'admin
<Agareth> non ci sto capendo molto.
<MaSTiFF> nn ho nulla chiedere passate al prox
<XSickBoyX> agareth che problema haI?
<IceCup> Non ho capito a cosa ci può servire la funzione trasferimento di zona
<MaSTiFF> :P
<IceCup> si possono avere più info
<IceCup> su di essa
<L3sus> neanche io come icecip
<XSickBoyX> col trasferimento di zona
<XSickBoyX> puoi avere info sulle makkine e i servizi che compongono una rete locale
<L0GAN> •Scusa una cosa, ma gli IP non arrivano fino a 255?
<Agareth> ah ecco

<Agareth> allora..
<L0GAN> •1:-)
<XSickBoyX> logan cghe ho scritto?
<SaNdStOrM> •0,12chi ha il + davanti può parlare, a turno lo diamo a tutti
<L0GAN> avevi scritto 256
<MisterX> mi da sempre unrecognized command
<XSickBoyX> oh gesù
<L0GAN> :-)
<L0GAN> fa nulla, era solo una conferma
<Agareth> sto
<XSickBoyX> misterx però nn provate tutto adesso
<Agareth> scaricando netlab, dopo che faccio?
<Puvio> Passo Grazie
<SaNdStOrM> •0,12chi ha il + davanti può parlare, a turno lo diamo a tutti
<MisterX> ok
<XSickBoyX> fai le varie interrogazioni whois x adesso
<SaNdStOrM> •0,12Chi ha il •+• davanti può parlare, a turno lo diamo a tutti
<XSickBoyX> altre domande?
<Agareth> uhm
<Agareth> ecco un secondo
<L0GAN> Ma chi è che ti faceva gli scan...
<XSickBoyX> un tipo con la tiscali
<L0GAN> con le porte dei trojan????
<XSickBoyX> si
<XSickBoyX> ne sai qualcosa?
<XSickBoyX> :)
<L0GAN> cacchio!!
<L0GAN> no, io ho tin.it
<Agareth> dopo aver 'scannato' con Netlab?
<XSickBoyX> agareth
<Sbirilindo> ok raga, di ke si parla
<XSickBoyX> tu i whois li usi semplicemente x prendere info sulla società
<Agareth> # ARIN WHOIS database, last updated 2003-09-30 19:15
<Agareth> # Enter ? for additional hints on searching ARIN's WHOIS database.
<s3xers> •io nulla da chiedere passate pure
<SaNdStOrM> •0,12Chi ha il •+• davanti può parlare, a turno lo diamo a tutti
<Sbirilindo> del netlab.......
<XSickBoyX> chi deve avere il + x kiedere qualcosa
<Agareth> allora come mai quel problema?
<XSickBoyX> mandate un pvt a me
<L0GAN> io ce l'ho il netlab, ma è una versione vecchia
<XSickBoyX> logan basta cercare
<Agareth> euhm
<Agareth> guarda:
<Agareth> google.it@whois.arin.net
<Agareth> mi esce:
<THEREDSOLDIER1988> nn ho nulla da chiedere
<XSickBoyX> chi ha bisogno del + mi mandi un pvt
<Agareth> # ARIN WHOIS database, last updated 2003-09-30 19:15
<Agareth> # Enter ? for additional hints on searching ARIN's WHOIS database.
<Agareth> come mai?
<XSickBoyX> agareth che client stai usando?
<Puvio> Non ho nulla da chiedere
<Agareth> 1.3
<|AliA[s]|> •non ho niente da chiedere•
<XSickBoyX> ice parloa
<XSickBoyX> ma netlab
<XSickBoyX> ?
<IceCup> ok grazie
<Bubble> Come faccio a trovare un IP da un indirizzo e-mail???
<Agareth> sì
<XSickBoyX> bubble ne parleremo più avanti
<Bubble> ok...
<XSickBoyX> agareth ha un'interfaccia grafica?
<XSickBoyX> prova ad inserire
<XSickBoyX> solo google.it
<Agareth> sì
<L0GAN> beh, credo che lo devi vedere quando ti mandano un messaggio col client

di posta
<XSickBoyX> POSSIAMO ANDARE AVANTI??????????
<Agareth> # ARIN WHOIS database, last updated 2003-09-30 19:15
<Agareth> # Enter ? for additional hints on searching ARIN's WHOIS database.
<Agareth> niente..
<XSickBoyX> metti ?
<XSickBoyX> e vedi che ti dice :)
<Agareth> mi escono un po' di cose
<XSickBoyX> altre domande??
<XSickBoyX> bene
<SaNdStOrM> •0,12Chi ha il ••12,0+••0,12• davanti può parlare e fare •domande inerenti alla lezione•, a turno lo diamo a tutti
<XSickBoyX> quel po di cose
<XSickBoyX> solo i comandi che puoi usare
<XSickBoyX> divertiti
<XSickBoyX> chi ha domande
<XSickBoyX> mandi un pvt ad alex
<Agareth> ma come divertiti..
<XSickBoyX> o a me
<XSickBoyX> o a sand
<AlexMessoMalex> ha ha ha
<XSickBoyX> ahahahahah
<XSickBoyX> s'è preso collera
<XSickBoyX> vabbè
<SaNdStOrM> riprendiamo?
<XSickBoyX> domande??????????
<SaNdStOrM> ok
<XSickBoyX> ok andiamo
<XSickBoyX> raga
<XSickBoyX> comunque
<XSickBoyX> io consiglio SamSpade
<XSickBoyX> x i whois
<XSickBoyX> www.samspade.org
<XSickBoyX> lo trovate lì
<XSickBoyX> passiamo
<XSickBoyX> ai traceroute
<XSickBoyX> cos'è il traceroute??
<XSickBoyX> è l'invio di un pacchetto "sonda"
<XSickBoyX> che ci dice x quali pc passa
<XSickBoyX> x arrivare ad un determinato ip
<XSickBoyX> mi spiego meglio
<XSickBoyX> facciamo il caso che io voglio comunicare con l'ip 10.10.10.1
<XSickBoyX> facciamo il caso che voglio sapere
<XSickBoyX> dove passano i miei pakketti prima di arrivare all'ip sopra
<XSickBoyX> ecco che uso il traceroute
<XSickBoyX> che
<XSickBoyX> sfrutta
<XSickBoyX> le proprietà TTL di un pakketto
<XSickBoyX> le proprietà Time To Live
<XSickBoyX> ok???
<XSickBoyX> x quelli che stanno arrivando adesso
<XSickBoyX> tutto verrà loggato
<XSickBoyX> adesso stiamo parlando dei traceroute
<XSickBoyX> vi siete persi i whois :)
<XSickBoyX> x Unix
<XSickBoyX> il traceroute
<XSickBoyX> lo troviamo un pò ovunque
<XSickBoyX> x winzozz molto carino
<XSickBoyX> visual route 7
<XSickBoyX> anche se io preferisco i client a riga
<XSickBoyX> danno maggiore soddisfazione :)
<XSickBoyX> allora
<XSickBoyX> facciamo praticamente un traceroute al sito pippo.com
<XSickBoyX> [bash] traceroute 10.10.10.1
<XSickBoyX> l'uotput dovrebbe essere una cosa del genere
<XSickBoyX> tracerouteto (10.10.10.1)
<XSickBoyX> 1gate (10.10.15.1) 993ms
<XSickBoyX> 2attrib.pippo.it (12.10.10.1)

<XSickBoyX> 3rtr.pippo.it (85.52.52.36)
<XSickBoyX> 4***
<XSickBoyX> 5***
<XSickBoyX> 6***
<XSickBoyX> allora
<XSickBoyX> prendiamo in analisi questo esempio
<XSickBoyX> il nostro ping è partito
<XSickBoyX> ed ha incontrato il pc gate (10.10.15.1 è il suo ip e 993ms è il ping)
<XSickBoyX> notate che 993ms l'ho messo solo
<XSickBoyX> su gate
<XSickBoyX> x questione di tempo ok?
<XSickBoyX> allora
<XSickBoyX> il secondo hop è su attrib.pippo.it
<XSickBoyX> il terzo su trt
<XSickBoyX> ect
<XSickBoyX> vediamo che al 4 ci stanno gli ***
<XSickBoyX> che cos'è?
<XSickBoyX> traceroute
<XSickBoyX> x default usa pacchetti udp
<XSickBoyX> ••2ciao sei un achers?•
<XSickBoyX> Ragazzi
<XSickBoyX> x favore
<XSickBoyX> no pvt
<XSickBoyX> allora
<XSickBoyX> probabilmente questa azieenda
<XSickBoyX> ha una
<XSickBoyX> ha un firewall che li blokka
<XSickBoyX> allora
<XSickBoyX> possiamo capire
<XSickBoyX> che il sistema è protetto
<XSickBoyX> almeno da un firewall
<XSickBoyX> visual route 7
<XSickBoyX> x win
<XSickBoyX> ha addirittura un interfaccia grafica chee vi dice la locazione dei vari pc
<XSickBoyX> anche se nn credo che sia attendibile
<XSickBoyX> ok
<XSickBoyX> andiamo con le domande
<XSickBoyX> chee nn sono molte
<XSickBoyX> immagino
<XSickBoyX> pvt a sandstorm chi ha domande da fare
<XSickBoyX> sand dai il voice solo a chi deve fare domande
<XSickBoyX> scusate se sono noioso ma vorrei fare qualcosa di completo
<XSickBoyX> Nessuna domanda??????????????????????????????
<AlexMessoMalex> il canale è moderato, non possono parlare
<AlexMessoMalex> facciamo una pausa per le domande?
<XSickBoyX> facciamo una cosa
<XSickBoyX> mandate un pvt
<XSickBoyX> ad alex
<XSickBoyX> se avete domande e lui vi dà il voice
<SaNdStOrM> ok
<AlexMessoMalex> ok, se volete parlare chiedetemelo in privato facendo doppio click sul mio nick
<SaNdStOrM> ora diamo lo spazio alle domande
<AndreaGeddon> posso chiedere?
<darkernel> ok
<XSickBoyX> si
<XSickBoyX> ditemi
<AndreaGeddon> se ci sono diversi hop tra il punto di partenza e arrivo
<AndreaGeddon> come fa un pacchetto a sapere dove andare?
<AndreaGeddon> cioè
<AndreaGeddon> pippo.com non è collegato a me direttamente
<XSickBoyX> beh ci sono degli indirizzamenti
<darkernel> io non o proprio capito perke' fare un trace
<XSickBoyX> no
<XSickBoyX> allora di solito
<XSickBoyX> funziona così

<XSickBoyX> io metto l'host cioè pippo.com
<XSickBoyX> l'info va a uno dei 13 (se nn erro) computeroni dove sta "scritto che l'host pippo.com si riferisce all'ip 10.10.10.1
<XSickBoyX> facciamo il caso
<XSickBoyX> che pippo.com sia protetto
<XSickBoyX> da un gateway
<darkernel> quindi serve solo per capire l'ip del sito
<darkernel> tutto questo
<XSickBoyX> allora le connessioni nn saranno dirette
<XSickBoyX> a lui ma prima al gateway ect
<XSickBoyX> no
<XSickBoyX> serve x capire x quali makkine passano i pakketti
<AndreaGeddon> al gateway?
<AndreaGeddon> si però
<AndreaGeddon> a sua volta
<AndreaGeddon> io posso non essere connesso direttamente al gateway?
<XSickBoyX> certo
<XSickBoyX> con una connessione diretta
<AndreaGeddon> e quindi siamo come prima
<AndreaGeddon> che devo sapere dove andare
<XSickBoyX> sennti
<XSickBoyX> il whois il traceroute e come vedremo i ping
<XSickBoyX> scusa stupido ma stiamo parlando di whois
<XSickBoyX> servono
<XSickBoyX> a capire
<XSickBoyX> un pò la struttura della rete
<XSickBoyX> se aspettate un pò vi sspiego
<XSickBoyX> come far interagire
<XSickBoyX> i whois
<XSickBoyX> i traceroute
<XSickBoyX> e i ping
<darkernel> ok
<nebbia> lo switch è molto + evoluto dell'hub
<XSickBoyX> x adesso nn ci interessando gli switch o gli hub
<XSickBoyX> domande?
<XSickBoyX> veloce
<XSickBoyX> che altrimenti ci mettiamo un casino di tempo
<darkernel> azz riavvio
<AlexMessoMalex> domande?
<darkernel> il pc impazzisce
<vmaster> ma ke state a fa?
<vmaster> scusate?
<XSickBoyX> DOMANDE??
<XSickBoyX> DOMANDE?????????????????
<XSickBoyX> potete scrivere tutti ora
<rolando> non ho capito nulla!
<HolySniper> dai andiamo avanti
<Sbirilindo> ok
<AndreaGeddon> beh non ho chiaro il fatto dei pacchetti
<Puvio> sigh
<XSickBoyX> rolando abbiamo parlato di whois e traceroute
<|AliA[s]|> continua korn
<kOrn[CsA]> come faccio a cambiare la rotta di un pacchetto una volta instradato?
<SaNdStOrM> sicuramente non ripete, rolando
<XSickBoyX> tu non la cambi
<Sbirilindo> sick posso spiegare la cosa dei pacchetti ke nessuno capisce
<XSickBoyX> vai sbirilindo
<Sbirilindo> allora
<rolando> spiega
<Sbirilindo> io inserisco l'IP
<Sbirilindo> 10.10.10.10
<Sbirilindo> il pacchetto arriva a 10.10.10.10
<Sbirilindo> e quando ritorna indietro mi dice per quali computeroni è passato
<Sbirilindo> es
<Sbirilindo> IO--->computerone1--->computerone2--->10.10.10.10
<Sbirilindo> capito qualcosa
<Sbirilindo> ki non ha capito mi faccia una domanda

<AlexMessoMalex> domande veloci che concludiamo
<Alkemico> come si buca la nasa?
<Alkemico> :°
<ShackaN> che cavolo ci faccio qui ??
<AlexMessoMalex> alkemico vuoi essere bannato?
<darkernel> di cosa si e' parlato in mia assenza
<Sbirilindo> con un trapano
<Sbirilindo> :)
<AndreaGeddon> sbi, si ho capito
<AndreaGeddon> mettiamo che
<anime|1000> sera
<AndreaGeddon> io -> a -> b -> c -> d -> sito.com
<Vega_> Sbirilindo: come avviene il tutto di preciso?
<AndreaGeddon> io mando il pacchetto che passa verso a
<XSickBoyX> azz
<XSickBoyX> raga
<XSickBoyX> scaricate
<AndreaGeddon> ma poi a come sa dove sta sito.com?
<XSickBoyX> un client traceroute
<XSickBoyX> e capirete subito
<Nyo`> ke palle
<AndreaGeddon> so come funziona il traceroute
<Nyo`> o l'ho potuto dire:)
<Dejavu> xsick...bella lezione si sto vedendo
<AndreaGeddon> so come traceroutare, ma non mi è chiaro il meccanismo interno
<Sbirilindo> con visual route te lo indica sulla cartina geografica
<Vega_> XSickBoyX: io intendo cosa accade realmente non gli effetti
<L0GAN> exactly
<darkernel> HO SCARICATO GENIUS
<darkernel> come client
<XSickBoyX> scusate
<XSickBoyX> allora ripeto tutto
<XSickBoyX> velocemente
<XSickBoyX> forse non sono stato chiaro
<XSickBoyX> il traceroute
<XSickBoyX> serve a capire la topologia e individuare i vari percorsi di accesso
<XSickBoyX> solo un attimo
<XSickBoyX> dopo le domande
<XSickBoyX> allora
<XSickBoyX> sia x win che x linux
<XSickBoyX> esiste il client
<XSickBoyX> traceroute
<XSickBoyX> che usiamo così
<XSickBoyX> traceroute ip_vittima
<XSickBoyX> il suo output sarà gli ip di tutti i pc dove passeranno i pacchetti
<XSickBoyX> come accade ciò?
<XSickBoyX> traceroute sfrutta le proprietà TTL (time to live) del pacchetto
<XSickBoyX> e così ci può dire il percorso che ffa x andare nel pc vittima
<XSickBoyX> se escono degli asterischi al posto dell'ip
<XSickBoyX> vuol dire che il traffico entrante x il pc vittima
<XSickBoyX> è filtrato
<XSickBoyX> da un firewall o qualcosa del genere ok????
<XSickBoyX> ki ha domande
<XSickBoyX> mi mandi un PVT
<XSickBoyX> o lomandi a SAND O A ALEX
<SaNdStOrM> poi andiamo avanti
<SaNdStOrM> e concludiamo la prima sera
<darkernel> ok
<darkernel> io faccio il trace
<AlexMessoMalex> c'è una domanda non risposta :
<AlexMessoMalex> <AndreaGeddon> so come traceroutare, ma non mi è chiaro il meccanismo interno
<darkernel> pure di un sito???
<XSickBoyX> si dark
<darkernel> esatto
<XSickBoyX> un sito sta cmq su un server
<darkernel> mi compaiono una lista di ip
<XSickBoyX> andrea

<anime|1000> se invece escono sempre gli ip?
<anime|1000> e mai gli ***?
<darkernel> con hostname ectt
<XSickBoyX> anime vuol dire che il traffico entrante
<XSickBoyX> non è filtrato
<darkernel> non non mi scnon
<darkernel> *escono gli ***
<XSickBoyX> il traceroute SFRUTTA
<XSickBoyX> le proprietà TTL
<XSickBoyX> da ogni router
<XSickBoyX> ogni router
<darkernel> time to live:D)))))
<XSickBoyX> da cui passa
<XSickBoyX> un certo pakketto
<anime|1000> come si fa a saltare i firewall o roba del genere?
<XSickBoyX> deve diminuire
<XSickBoyX> aspe
<XSickBoyX> stop
<XSickBoyX> anime
<XSickBoyX> una cosa alla volta
<darkernel> ma in numeri cosa signifikano rt???
<darkernel> RT
<XSickBoyX> rt???
<darkernel> si
<XSickBoyX> cos'è rt?
<darkernel> rt(MS)
<active85k> act
<darkernel> E' IL TEMPO DEL PAKKETTO
<active85k> io ho fatto una domanda
<active85k> ...
<active85k> la scrivo in chan?
<XSickBoyX> si
<Sciac4llo> Aspè..
<XSickBoyX> scusa active
<Vega_> XSickBoyX: scusa...che intendi per sfrutta le propieta TTL....cosa accade in pratica
<XSickBoyX> ma NON RISP A PVT
<Sciac4llo> XSickBoyX, voglio farti una domanda.
<XSickBoyX> ok ve lo spiego subito
<active85k> ******************************
<active85k> [22:23] <active85k> io ho una domanda
<active85k> [22:23] <active85k> riguarda un one byte buffer overflow
<active85k> [22:23] <active85k> la domanda è la seguente:
<active85k> [22:24] <active85k> per eseguire un attacco di questo genere, quali condizioni devono verificarsi all'interno dell'applicazione "vittima" per consentire il mio attacco? e quali sono i casi + evidenti?
<active85k> **
<Sciac4llo> come si calcola il campo cheksum dell'header udp
<Sciac4llo> come si calcola il campo cheksum dell'header udp
<Sciac4llo> ?
<XSickBoyX> FERMI
<XSickBoyX> CAZZ
<darkernel> :s
<darkernel> AZZ
<XSickBoyX> allora
<XSickBoyX> sciacallo
<Sciac4llo> Si?
<Vega_> si ma che senso ha fare mille domande..ora si parla di una cosa...basta...solo di quello no?
<XSickBoyX> che c'entra il check sum adesso????
<Vega_> torniamo al traceroute
<Vega_> per favore
<XSickBoyX> active non stiamo parlando di buffer overflow
<darkernel> torniamo con trace ectt...
<XSickBoyX> na cosa alla volta ok?
<Sciac4llo> E un' altra cosa..
<XSickBoyX> allora
<XSickBoyX> brevemente spiego il meccanismo

<XSickBoyX> del traceroute
<XSickBoyX> allora traceroute
* SaNdStOrM sets mode: +b *!*@Azzurra-15232616.tnt2.mln4.ita.da.uu.net
<XSickBoyX> sfrutta la proprietà TIMETOLIVE del pakketto IP per ottenere un messaggio ICMP TIME_EXCEEDED da ogni router
* Sciac4llo was kicked by SaNdStOrM (va a da via 'l cu ti, il cheksum e l'header udp•)
* SaNdStOrM sets mode: +b *!*@Azzurra-4E42DE2.pool80117.interbusiness.it
<XSickBoyX> visto che ogni router attraversato dal pakketto
* stupido_idiota was kicked by SaNdStOrM (va a da via 'l cu ti, il cheksum e l'header udp•)
<XSickBoyX> deve diminuire il valore
<XSickBoyX> del campo TTL
<XSickBoyX> questo diventa a tutti gli effetti un "contatore di salti (HOP)
<XSickBoyX> e proprio sta cosa
<XSickBoyX> ci permette di usare i clients traceroute
<XSickBoyX> x stabilire il percorso esatto
<XSickBoyX> A che serve il traceroute
<XSickBoyX> ???
<XSickBoyX> serve ad identificare eventuali dispositivi di controllo
<XSickBoyX> firewall hardware o software
<XSickBoyX> o router con filtri su pakketti
<XSickBoyX> ok???
<XSickBoyX> dove trovare il client traceroute???
<XSickBoyX> aspettate
<XSickBoyX> che ho un quadernino dovestanno scritti i link
<XSickBoyX> x i vari progr
<XSickBoyX> allora
<XSickBoyX> x win c'è www.visualroute.com
<XSickBoyX> o potete usare NeoTrace
<XSickBoyX> www.neotrace.com
<XSickBoyX> x linux
<XSickBoyX> il programma traceroute
<XSickBoyX> lo dovreste trovare qui
<XSickBoyX> ftp://ftp.ee.lbl.gov/traceroute.tar.Z
<XSickBoyX> allora
<XSickBoyX> ultime domande
<XSickBoyX> e poi
<XSickBoyX> anticipo gli scan
<XSickBoyX> e poi ci si vede domani sera
<AlexMessoMalex> senza scaricare un programma, in Windows avete il TRACERT, è sufficiente che andiate in promt di ms-dos e scriviate "tracert" (senza virgolette)
<Vega_> allora quello che vorrei capire
<Vega_> è come in effetti
<Vega_> si contano gli hop..
<Vega_> cosa accade...
<Vega_> inoltre per linux non credo che ci sia bisogno
<Vega_> un mio amico
<Vega_> mi pare mi abbia detto
<dark87> XSickBoyX ke firewall mi consigli????risp cazzo!!!!!
<Vega_> che è gia incluso no?
<dark87> XSickBoyX ke firewall mi consigli????risp cazzo!!!!!
<dark87> XSickBoyX ke firewall mi consigli????risp cazzo!!!!!
<dark87> XSickBoyX ke firewall mi consigli????risp cazzo!!!!!
<anime|1000> come si impostano i ttl in tracert?
<active85k> ********************
<active85k> ma con un traceroute di quel tipo là, non è possibile attaccare un server con post-desincronizzazione passiva del server stesso in quanto noi non siamo direttamente in rete. C'è un modo per prendere i pacchetti senza esserci fisicamente in mezzo?
<active85k> *************************
* dark87 was kicked by SaNdStOrM (prova te a rispondere a tutti contemporaneamente.... con calma•)
* dark87 has joined #AlexMessoMalex
* SaNdStOrM sets mode: +v dark87
<Sbirilindo> signori rifatemi tutte le domande
<Vega_> XSickBoyX: chiaro il mio quesito?

<dark87> XSickBoyX ke firewall mi consigli????risp cazzo!!!!!
<Sbirilindo> rispondo io
<XSickBoyX> dark uso blackice e a volte zonealarm
<XSickBoyX> si vega
<XSickBoyX> traceropute in linux già c'è
<Vega_> ok..
* SaNdStOrM sets mode: -v dark87
<Sbirilindo> allo il firewall zone alarm
<Vega_> oltre a quello che è il minimo..
<Vega_> mi piacerebbe capire
<XSickBoyX> vega in che senso si contano gli op??
<Vega_> come in effetti
<XSickBoyX> allora
<Vega_> cosa accade
<Vega_> dire che usa
<Vega_> il ttl
<Vega_> nn mi chiarisce quello che avviene :(
<Sbirilindo> allora
<Vega_> vorrei capire
<Sbirilindo> asp
<Vega_> una sessione minima
<anime|1000> una domanda ma ogni quanto ci sono queste lezioni ed a che ora?
<active85k> scusate un sec... ma un firewall alle volte, se preso di mira da un cracker, non potrebbe addirittura facilitare l'apertura di una porta sul pc? che alla fine il programma per controllare gli attakki le porte le apre... è così?
<Sbirilindo> se stai capma ti spiego
<Sbirilindo> calma....
<XSickBoyX> animel
<XSickBoyX> decidiamo fra poco
<Sbirilindo> vega
<anime|1000> fra poco?
<Sbirilindo> allora
<XSickBoyX> si
<Sbirilindo> il TTL
<active85k> :(
<Vega_> dimmi Sbirilindo
<XSickBoyX> ragazzi che dite vado avanti??????
<XSickBoyX> o ci vediamo la prox volta????????
<active85k> ma io ho fatto 2 domande :(
<Sbirilindo> allora il TTL
<darkernel> scarikati come firewall kerio
<Sbirilindo> gli hop si calcolano
<Sbirilindo> con il TTL
<XSickBoyX> active x la tua ultima domanda
<XSickBoyX> non sono sicuro
<XSickBoyX> un firewall non apre le porte x controllarle
<Sbirilindo> ogni volta ke il pacchetto passa x i computeroni
<XSickBoyX> ma è motlo facile
<t> buonasera, domandina: qualcuno potrebbe spiegarmi come, quando e in base a quali politiche viene effettuata la fragmentation dei pacchetti ?
<XSickBoyX> che nn controlli alcuni tipi di ping
<XSickBoyX> azz
<XSickBoyX> t
<XSickBoyX> hai fatto una domanda
<Vega_> come Sbirilindo....questo vorrei capire..come se li segna..
<Vega_> gli ip
<Vega_> di ogni "computerone"
<Sbirilindo> i computeroni scalano un valore, il valore del TTL
<XSickBoyX> che ci vorrebbe buono dieci min x risponderti
<active85k> e allora il firewall in base a cosa si rende conto che arrivano dati senza aprire la porta? non mi sembra che winsock.dll dia una possibilità di questo tipo (prendendo windows come esempio)
<t> XSickBoyX: ho tutto il tempo che vuoi
<Sbirilindo> vega in PVT
<active85k> nessuno?
<XSickBoyX> active
<XSickBoyX> quando ricevono un ping
<active85k> si...

<XSickBoyX> o qualcosa
<XSickBoyX> a seconda del ping o della richiesta
<XSickBoyX> possono rispondere
<XSickBoyX> o no
<active85k> ma se la porta è chiusa i dati non vengono proprio notificati
<XSickBoyX> come vedremo nella prossiamo spiegazione
<active85k> l'handler non analizza alcuna richiesta
<active85k> cioè... come è possibile
<active85k> che un firewall riesca a prendere dei dati
<active85k> in quel caso specifico?
<active85k> in effetti un solo utente per 46 persone mi sembra un po' eccessivo
<XSickBoyX> ho duemila
<XSickBoyX> richieste in pvt
<active85k> 60 query...
<XSickBoyX> siamo arrivati al traceroute
<korn\mate> oh
<Rasta`][v][an> Hi All =o)
<darkernel> .
<Demon> CIAO ALEX
<Rasta`][v][an> scommetto ke sono arrivato tardi?
<HolySniper> partendo dall'whois
<L0GAN> raga devo andare
<L0GAN> torno domani
<Nyo`> o me che palle, me ne vado, ciao
<Vega_> cmq sia
<HolySniper> sick potresti andare avanti col prossimo argomento?
<XSickBoyX> RAGAZZI Ultima
<XSickBoyX> cosa
<XSickBoyX> se vi va bene
<XSickBoyX> la prox lezione
<XSickBoyX> si terrà domani ALLE 22
<XSickBoyX> grazie x l'attenzione
<XSickBoyX> x stasera abbiamo finito
<anime|1000> un pò più tardi!
<mainman> arrivo sempre troppo tardi
<Rasta`][v][an> co due
<darkernel> e' finito:))))))))))99
<bellintri> ciao
<korn\mate> gh
<Vega_> ma in pratica..
<Rasta`][v][an> di ke avete parlato oggi?
<korn\mate> apt su slack nn funz
<korn\mate> apt su slack nn funza
<Vega_> che avreste spiegato..
<Vega_> mika l'ho capito...
<L0GAN> Raga io vado
<kOrn[CsA]> addio
<korn\mate> bella korn
<korn\mate> ;D
<Rasta`][v][an> mi raccomando nn accalcatevi
<kOrn[CsA]> salve korn
<Rasta`][v][an> uno alla volta
<AndreaGeddon> ciao a tutti
<Sbirilindo> ciao raga
<XSickBoyX> RAGA x curiosità
<kOrn[CsA]> lo so
<XSickBoyX> commenti sulla lezione????
<XSickBoyX> NOIOSA?
<kOrn[CsA]> korn: complimenti per il nick ^^
<Rasta`][v][an> qualcuno mi sa dire di cosa avete parlato questa sera?
<korn> lol korn
<korn> anke a te
<kOrn[CsA]> olè
<korn> ;)
<kOrn[CsA]> MD
<kOrn[CsA]> ;D
<ShackaN> lezione ? quale lezione ?
<AlexMessoMalex> •4,0COMUNICAZIONE IMPORTANTE •11,2il prossimo meeting si terrà

domani sera alle ore 22
<XSickBoyX> ahahahaha
<active85k> di cosa si parlerà?
<badboy84> <kOrn[CsA]> korn: complimenti per il nick ^^ <--------mai visti due scemi in una volta
<badboy84> lol
<anime|1000> più tardi please
<korn> badboy
<kOrn[CsA]> prot badboy
<Rasta`][v][an> qualcuno mi sa dire di cosa avete parlato questa sera?
<Sbirilindo> trovi tutto sul sito domani
<XSickBoyX> raga IO VADO
<Rasta`][v][an> azz la voglia di scrivere
<XSickBoyX> VI RINGRAZIO DELL'ATTENZIONE
<active85k> prego :)
<XSickBoyX> E SPERO CHE ABBIATE APPREZZATO
<HolySniper> grazie a te sick
<Sbirilindo> ha ha
<XSickBoyX> DOMANI PARLIAMO DI PING SCANNER
<XSickBoyX> E CIò CHE RIUSCIAMO A FARE
<AlexMessoMalex> Ragazzi, noi ci mettiamo la nostra volontà per organizzare questi eventi, speriamo vi siano graditi
<XSickBoyX> A DOMANI ALLE 22
<darkernel> graxie sick
<active85k> •a proposito... ho una cosa da proporvi
<active85k> per comodità
<anime|1000> un pò più tardi delle 22 si può fare?
<kOrn[CsA]> •dicci active
<Rasta`][v][an> XSickBoyX di ke avete parlato questa sera?
<Guest89589> buona serata
<XSickBoyX> RASTA DI WHOIS E TRACEROUTE IN AMBIENTE WIN E UNIXLIKE
<Rasta`][v][an> ok grazie mille =o)
<darkernel> domani ke argomento si tratterra????????
<AlexMessoMalex> anime|1000 purtroppo dobbiamo accontentare tutti, le 22 mi sembra un orario di compromesso
<anime|1000> :(°
<darkernel> DOMANI KE ARGOMENTO SI TRATTERA?????
<XSickBoyX> PING E SCANNER
<XSickBoyX> E CIò CHE RIESCO A FARE
<anime|1000> i vari tipi di scanner
<anime|1000> syn scann
<anime|1000> ecc...
<kOrn[CsA]> olè
<GGGG> AlexMessoMalex ma da quanti anni hai quel sito?
<baSheR> mi hai chiamato qualcosa ?
<anime|1000> try hander-schake
<baSheR> [anime|1000] try hander-schake <----- ok???
<baSheR> :/
<anime|1000> sbagliato a scrivere
<XSickBoyX> CIAO A TUTTI A DOMANI!!!!!!
<darkernel> CIAO SICKKKKKK