<AlexMalex> Iniziamo spiegando il concetto di NUKE per chi ancora fosse inesperto.
<AlexMalex> Un NUKE è un programma che invia moltissimi pacchetti di errore a un computer remoto intasandogli la connessione.
<AlexMalex> Lo scopo del NUKE è quello di spedire talmente tanti bytes da usare tutta la banda
<AlexMalex> di cui dispone la vittima al fine di impedirle di ricevere altre informazioni.
<MaRCo> sfrutta in pratica i bug di rete del sistema operativo
<AlexMalex> I migliori NUKES sono in grado di rendere inutilizzabile la connessione del computer remoto
<AlexMalex> tanto da indurre la vittima a disconnettere il modem dalla rete.
<MaRCo> lo scopo minimo è di sconnettere la vittima dal server irc a cui è connessa
<AlexMalex> Ovviamente l'efficienza di un NUKE dipende molto dalla connessione di chi
<AlexMalex> lo usa e da quella di chi lo subisce.
<AlexMalex> Se si usa un NUKE un comune modem analogico 56K verso una vittima con una ADSL 640K difficilmente si riuscirà
<MaRCo> più la connessione è stabile e veloce, più pacchetti possiamo inviare
<AlexMalex> ad ottenere ciò che si vuole, in ogni caso le si provocherà un certo fastidio.
<AlexMalex> In IRC si usano i NUKES per disconnettere un utente dalla chat.
<AlexMalex> La sua connessione con l'IRC Server cadrà come un caco maturo :-))
<MaRCo> chiaramente se gli fate cadere la connessione cadrà anche dalla chat
<AlexMalex> Il modo per difenderci dai NUKES è l'utilizzo di un firewall.
<MaRCo> però un nuke può far cadere un utente della chat senza necessarriamente sconnetterlo da internet
<AlexMalex> Un firewall è un programma che monitorizza le porte della vostra connessione.
<AlexMalex> MARCO vi spiegherà brevemente come agisce il PC Conseal firewall che potete scaricare nella sezione mIRC.
<MaRCo> un firewall molto diffuso è il ConSeal PC
<MaRCo> l'ultima versione è disponibile sul nostro sito
<MaRCo> dovete configurarlo un attimino
<MaRCo> i firewall vanno configurati affinchè blocchino gli attacchi in ingresso e non quelli in uscita dal vostro pc
<MaRCo> ci sono le cosiddette RULES (regole) che ogni volta il firewall carica affinche possa proteggervi
<MaRCo> Ad ogni tentativo di connessione o di attacco il nostro FW ci avvertirà e cercherà di sventarlo
<MaRCo> Ci avvertirà indicandoci l'ip dell'aggressore, la porta usata e il tipo di attacco/connessione
<MaRCo> e lo fermerà chiudendo quella porta questo a livello teorico
<MaRCo> poi dipende dalla qualità del firewall utilizzato e soprattutto dal tipo di attacco che vi fanno
<MaRCo> perchè in questo campo l'attacco è sempre migliore della difesa
<MaRCo> esistono nuke molto potenti e quindi non è che un firewall ci metta proprio al sicuro 100%
<MaRCo> sicuramente è meglio di niente, anche perchè se cadremo ugualemente, almeno sapremo l'ip di chi ci ha fatto sconnettere
<MaRCo> comunque occuppiamoci dell'attacco :)
<AlexMalex> Il VENOM script contiene diversi NUKES, il migliore dei quali è il CLICK
<MaRCo> in giro su internet, in ogni modo, si trovano un infinità di nuke, basta solo avere il tempo per "testarli"
<AlexMalex> Per nukkare un utente dovete cliccare sul suo nick con il tasto destro e
<MaRCo> il venom diciamo che ha il suo interno alcuni nuke e che ne automatizza la configurazione per eseguire l'attacco
<AlexMalex> Per nukkare un utente dovete selezionare un utente, cliccare sul suo nick con il tasto destro e
<AlexMalex> scegliere WAR Stuff - CLICK
<AlexMalex> In questo modo il VENOM automatizza la fase di compilazione dei campi CLIENT e SERVER del CLICK e lo esegue.
<AlexMalex> Per usarlo manualmente dovete invece fare un WHOIS a un utente

(/whois nickname),
<AlexMalex> leggere l'IRC server a cui è connesso e il suo IP (o host)
<AlexMalex> e compilare i campi SERVER e CLIENT rispettivamente con queste due informazioni (IRC Server e IP o host)
<MaRCo> ovviamente ciò che dovete nukkare è il client
<MaRCo> quindi dite al CLICK di inviare i pacchetti al client
<AlexMalex> Il programma CLICK è riconosciuto dagli antivirus come trojan quindi dovete
<AlexMalex> disabilitare il vostro antivirus quando lo usate.
<AlexMalex> Se la vittima è sprovvista di firewall dopo pochi secondi cadrà con "connection reset by peer"
<MaRCo> a meno che voi usiate windows e la vittima unix o mac il nuke non dovrebbe andare bene
<AlexMalex> Se non avete firewall per capire se vi stanno nukando, potete aprire le proprietà della connessione
<AlexMalex> facendo doppio click sull'iconcina che vi si apre quando vi connettete nella tray area di Windows (in basso a destra)
<AlexMalex> vedrete i bytes ricevuti che saliranno con una velocità abnorme (circa 10K/sec con una connessione 56K analogica)
<MaRCo> ad ogni modo ora riepilogo una cosa
<MaRCo> come nukare col venom usando ciò che mette a disposizione :
<MaRCo> selezionate un nick dalla lista col tasto sinistro
<MaRCo> ci cliccate sopra col destro
<MaRCo> sempre a quel nick o comunque ad uno della lista (l'importante è che prima abbiate selezionato col sinistro la vostra vittima)
<MaRCo> vi compare il solito menu, scegliete WAR STUFF
<MaRCo> troverete un po' di nuke tra cui il click
<MaRCo> (ma anche altri tipo assault icmp ecc...)
<MaRCo> per provarli soliti server della rete ircgate :))
<MaRCo> magari nel canale #lunapop :))
<MaRCo> nukando da qui il venom li compila in automatico mettendo lui l'ip e il server irc della vittima
<MaRCo> si può caricare anche una specie di console apposta per i nuke
<MaRCo> per farlo dal menu del venom scegliete Siege of Darkness
<MaRCo> da li Quick menu/option e poi venom war menu
<MaRCo> troverete i 6 nuke inclusi nel venom che però qui dovrete configurare voi
<MaRCo> non è difficile, bisogna sempre immettere l'ip/host della vittima
<MaRCo> (in alcuni casi basta quello come ad esempio il VTJ BOMBER)
<MaRCo> altri richiedono il server irc
<MaRCo> ma comunque sono informazioni che con un whois potete tranquillamente reperire
<MaRCo> a volte si preferisce usare un solo nuke come ad esempio il CLICK
<MaRCo> aumentando il numero di pacchetti di errore che invia e puntare tutto su quell'unico nuke
<MaRCo> a volte invece si possono utilizzare 2 o piùù nuke in contemporanea
<MaRCo> questo ovviamente rallenterà la vostra connessione correndo il rischio di cadere voi stessi
<MaRCo> dipende tutto da che connessione avete
<MaRCo> per capire i vostri limiti l'unico modo è quello di fare delle prove
<MaRCo> 2000/12/13 22.33.53 GMT +0100: Dispositivo di Co..[0000][No matching rule] Blocking incoming TCP: src=213.45.221.116, dst=213.45.151.118, sport=1586, dport=12345.
<MaRCo> come vedete da quello che ho incollato il firewall ci dice l'ip di chi ci sta facendo qualcosa (src) e l'ip nostro (dst)
<MaRCo> la porta di destinazione è quella che ci interessa (dport) ed essendo la 12345 è quella del netbus