GARR-CERT

servizio sicurezza GARR

Sicurezza in Ambiente Windows

III Incontro di GARR-B

(Firenze, 24-25 Gennaio 2001)

Andrea Pinzani

andrea.pinzani@fi.infn.it

INFN *Sezione di Firenze*

Le due famiglie Windows

- Windows 3.1
- Windows 95/98
- Windows ME

- Windows NT 3.51
- Windows NT 4
- Windows 2000

Acronimi

- SP Service Pack 1-2-3-4-5-6a
- KB Knowledge Base Microsoft
- SAM Security Account Manager
- LSA Local Security Authority
- SMB Server Message Block
- CIFS Common Internet File System
- DS Directory Service (Active Directory)
- LDAP Lightweight Directory Access Protocol
- IDS Intrusion Detection System
- DoS Denial of Service

GARR-CERT
servizio sicurezza GARR

Argomenti trattati

- Enumerazione Risorse
- Sicurezza in Windows 95/98
- Sicurezza in Windows NT/2000

Enumerazione Risorse (1)

- Scansione ed enumerazione
- Informazioni enumerate:
  - Risorse e condivisioni di rete
  - Utenti e gruppi
  - Applicazioni e Banner
- NT è il migliore amico dell'enumeratore

Enumerazione delle Risorse (2)

- net view
- Tools del Resource Kit
- DumpACL (DumpSec) di Somarsoft
- nbtstat –A 192.168.1.2 (utenti e gruppi)
- Scanner NetBIOS
- sid2user e user2sid

Connessione nulla
(Anonymous connection, red button vulnerability)

```
net use \\server\IPC$ "" /user:""
```

```
Net view \\server
Shared resources at \\192.168.1.2
SERVER
Share name  Type        Used as  Comment
-------------------------------------------------
NETLOGON    Disk                 Logon server share
Test        Disk                 Public access
The command completed successfully.
```

Contromisura: RestrictAnonymous

- Dal SP3 in poi
- Tramite `regedt32` modificare la chiave del Registry:

  `HKLM\SYSTEM\CurrentControlSet\Control\LSA`

  Selezionare `Edit -> Add Value`:

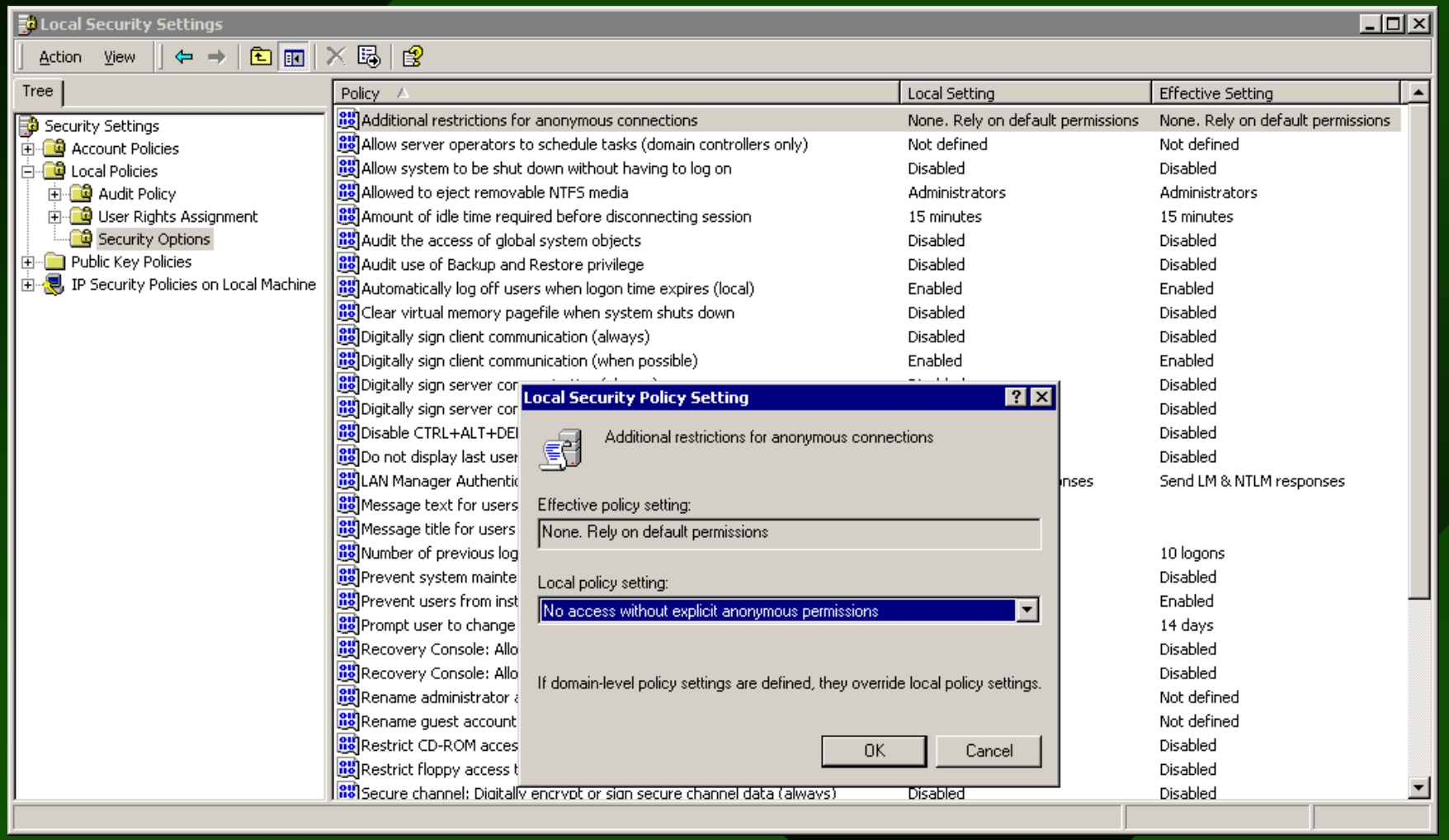
  `Value name:` **`RestrictAnonymous`**

  `Data Type:` **`REG_DWORD`**

  `Value:` **`1`** `(o` **`2`** `su Win2000)`

- Articolo Q155363 della Knowledge Base

Contromisura per Windows 2000

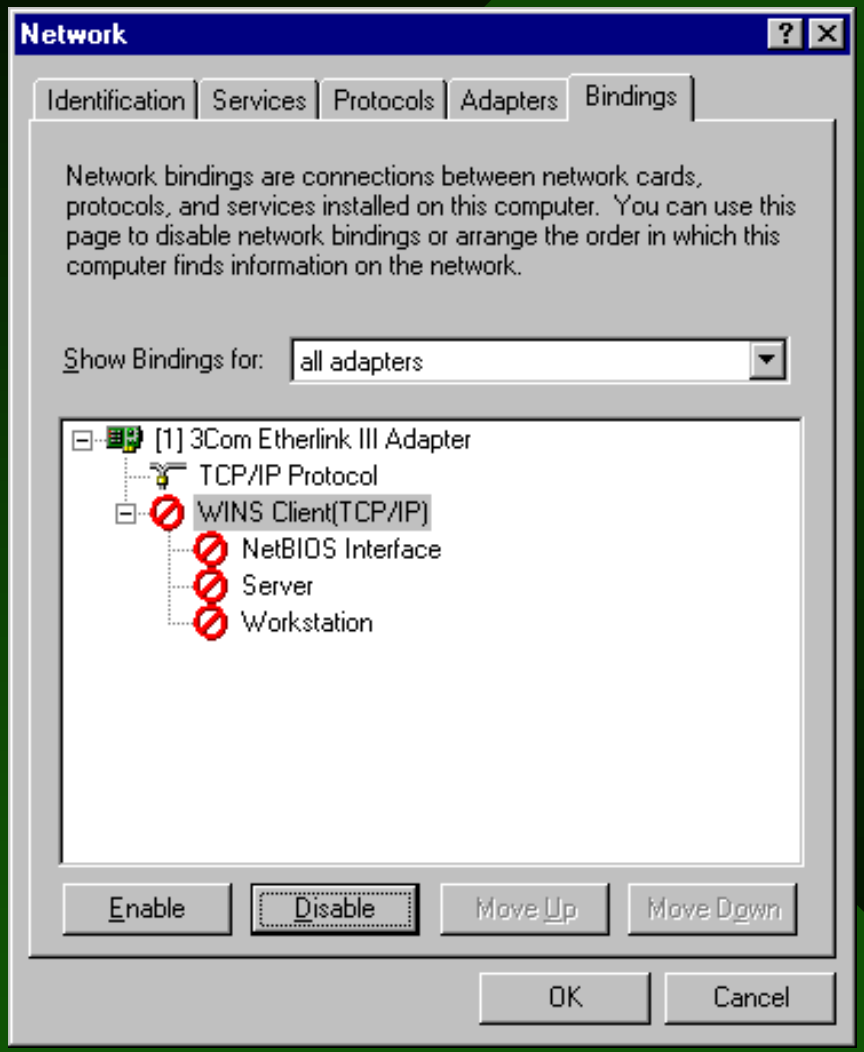


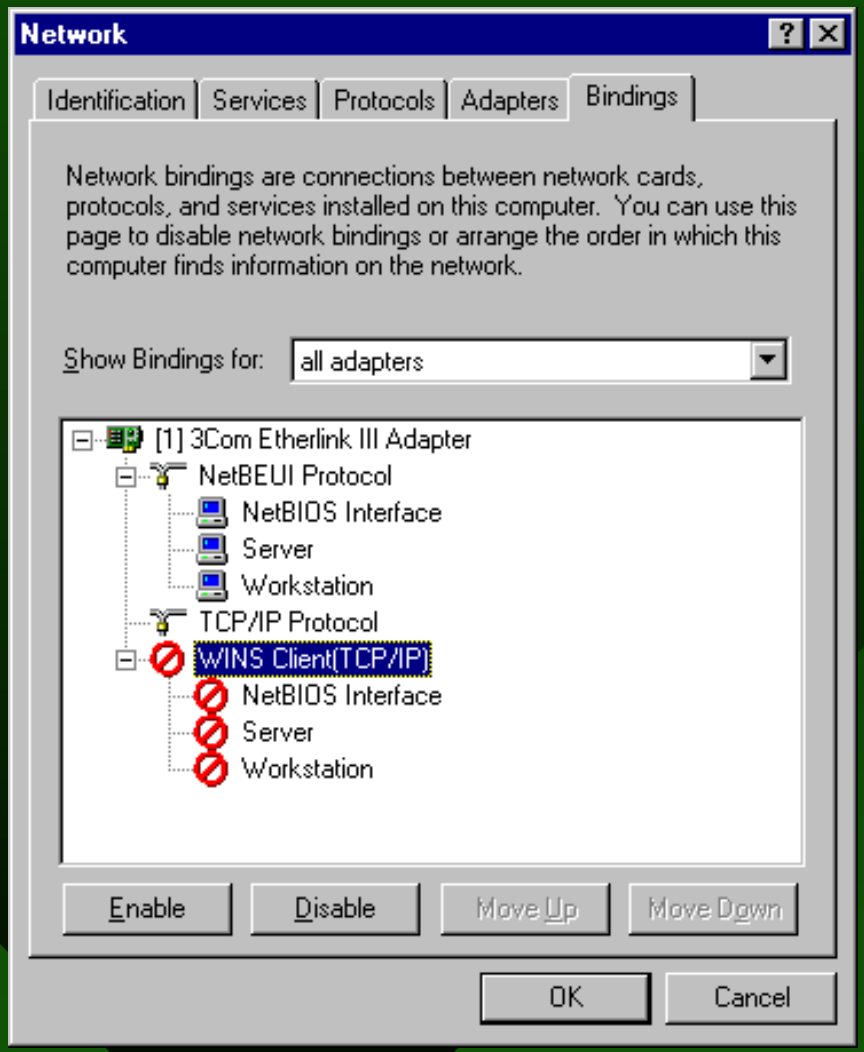
GARR-CERT
servizio sicurezza GARR

Protezione Condivisioni (1)

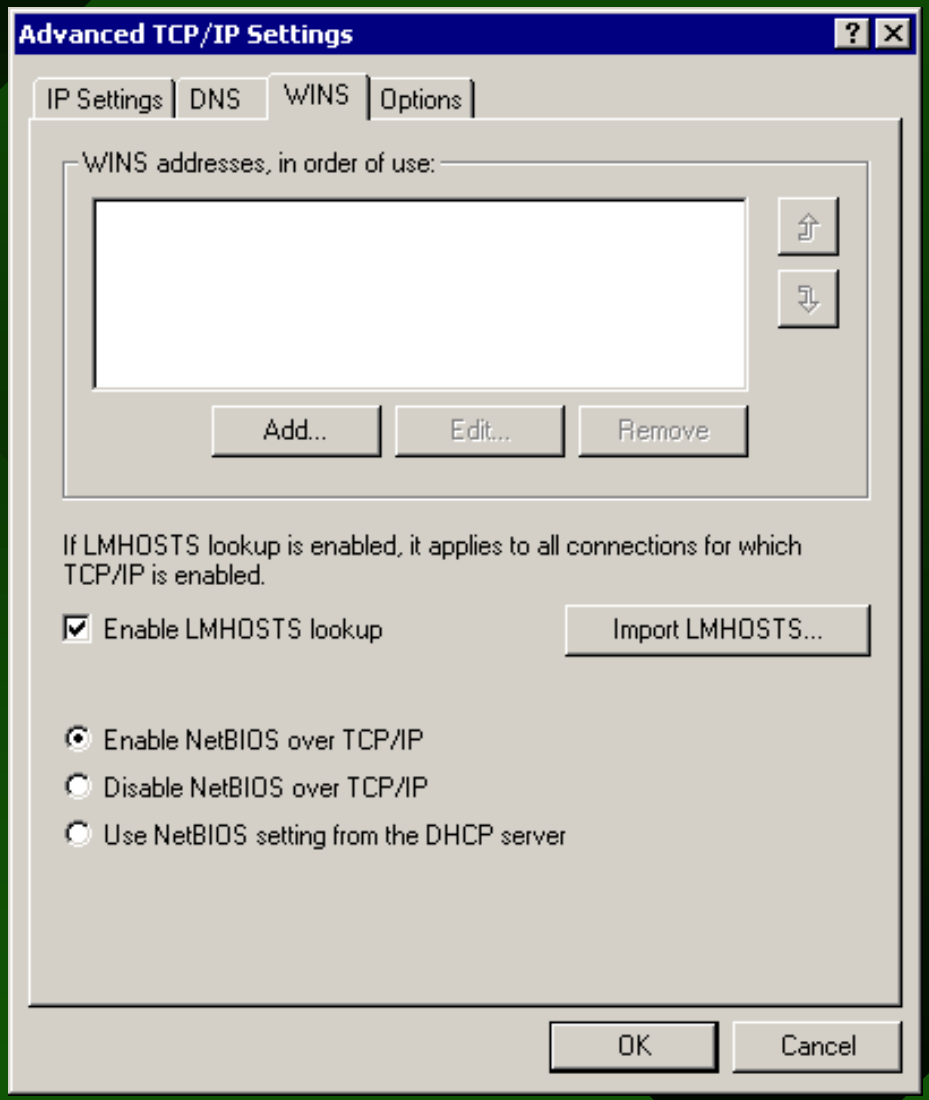
- Filtrare le porte TCP e UDP da 135 a 139
  (per Windows 2000 anche la 445)
- Disattivare il Binding del Wins Client (TCP/IP)
- Usate NetBEUI sulla rete locale

Protezione Condivisioni (2) Win NT





Protezione Condivisioni (3) Win 2K



Enumerazione di applicazioni e banner

- telnet su porte 21 (ftp), 25 (smtp) e 80 (http)
- Lettura Registry da Remoto (regdmp e DumpACL)

Contromisure:

- Assicuratevi che il Registry sia bloccato:

  `HKLM\SYSTEM\CurrentControlSet\SecurePipeServer\winreg`

  articoli Q143474 e Q155363

Agente SNMP

- Impostare una community non “public”
- Posizionarsi sulla seguente chiave del Registry:

```
HKLM\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\
ValidCommunities
```

impostare `Security -> Permission`

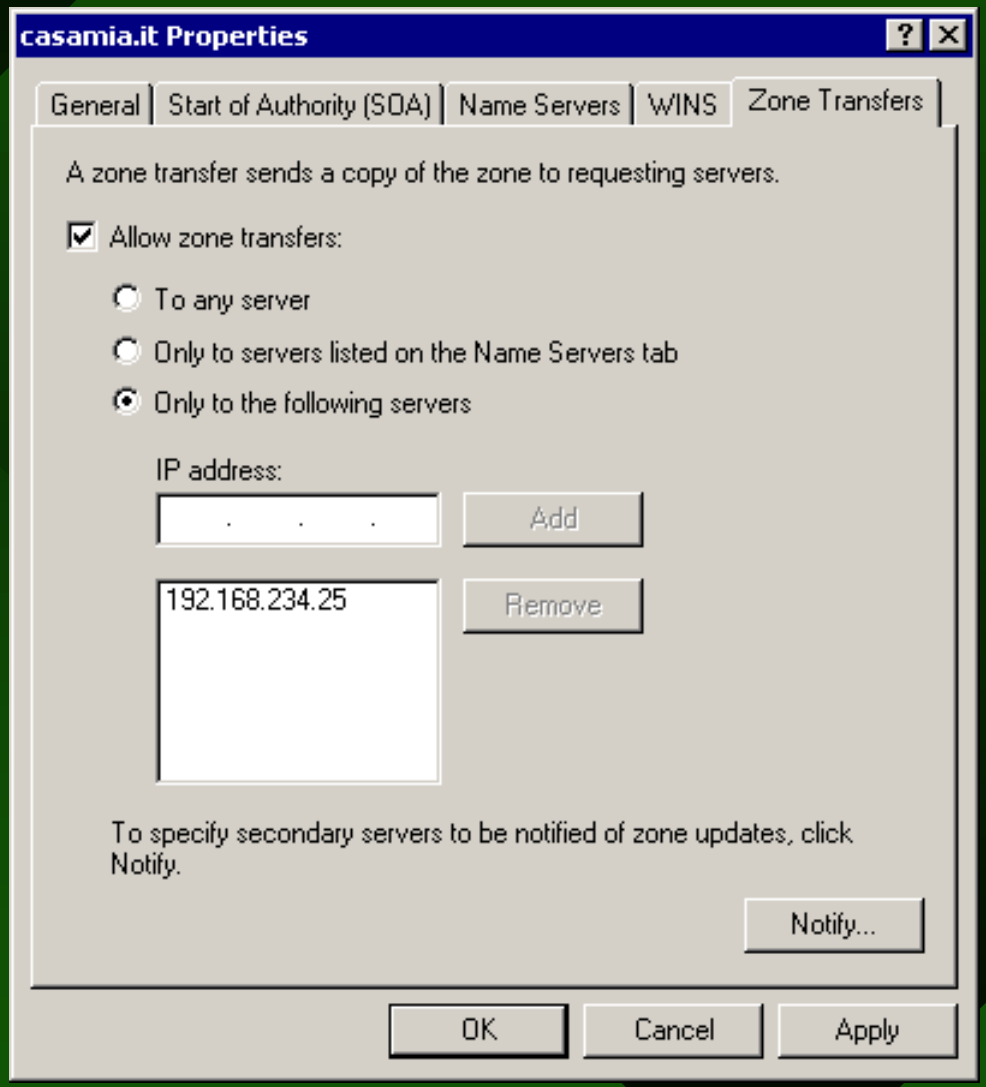
- Posizionarsi sulla chiave:

```
HKLM\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\
ExtensionAgents
```

eliminate il valore contenente la stringa `LanManagerMIB2Agent`

- Filtrate le porte TCP e UDP 161 (snmp) e 162 (snmp-trap)

Win 2000 DNS Zone Transferts



Sicurezza in Windows 95/98

- Semplicità contro Sicurezza
  - Monoutente
  - Multitask cooperative
- Controllo di accesso:
  - a livello utente
  - a livello di condivisione

Tipi di Attacco (da remoto) (1)

- Connessione diretta ad una condivisione
  (comprese le risorse di accesso remoto)

2. Installazione di un software trojan che apre una backdoor
3. Attacco tramite exploit di applicazioni server
4. Denial of Service

Tipi di Attacco (da remoto) (2)

Connessione diretta ad una condivisione

- Hacking delle cartelle condivise
  - Non attivate la condivisione File
  - Password robuste
  - Non condividere l'ntero disco
  - Condividere solo in lettura, o con password
  - Aggiungere $ al nome condivisione
  - Installate Analizzatore di rete
  - System Policy Editor (Resouce Kit)
- Hacking dei server di Accesso Remoto
  - Impostare password e cifratura
  - Oppure autenticare attraverso server NT
- Alterazione remota del Registry

Tipi di Attacco (da remoto) (3)

Installazione di trojan

- Back Orifice, Netbus ecc.
- Vanno installati esplicitamente:
  - Exploit di un applicazione client internet
  - Travestimento

Difese:

- Aggiornare i client internet e configurarli
- Programmi antivirus o prodotti specifici

Tipi di Attacco (da remoto) (4)

Exploit di applicazioni server

Difetti progettuali o strutturali del Sistema operativo o di applicazioni possono essere sfruttati. Esempi:

- Personal Web Server (non aggiornato)
- Alcuni Server FTP di vari produttori

Tipi di Attacco (da remoto) (5)

Denial of Service (windows 95/98)

- Winnuke, Ping of death, Land ecc.

Difese:

- Per Windows 95 installare DUN 1.3

Crack dei file PWL

- Cache delle password
- Algoritmo debole prima di OSR2

Difese:

- Disabilitare il caching tramite POLEDIT:

```
HKLM\SYSTEM\Microsoft\Windows\CurrentVersion\Policies\Network\
  DisablePwdCaching=1
```

Riepilogo

La minaccia più rilevante alla sicurezza di Windows 95/98 è l'esposizione delle cartelle condivise.

Quindi:

- Scegliere password accurate
- Uggiungete il simbolo $ al nome risorsa
- Filtrate le porte da 135 a 139
- Aggiornate Windows 95 con DUN 1.3

Sicurezza in Windows NT/2000

- Non prevede il lancio di processi da remoto (possibile con Terminal Server o tool specifici)
- Login da console ristretto (Non su NT workstation)
- Sorgenti non disponibili

Punti deboli:

- Compatibilità verso sistemi DOS
- Scelte fatte per semplificarne l'uso
  (protocolli NetBIOS/CIFS/SMB e hash LanManager)

Obbiettivi perseguiti dall'hacker

- Ottenere i privilegi di Administrator
- Consolidare il potere ottenuto
- Coprire le proprie tracce

Attacco all'utente Administrator

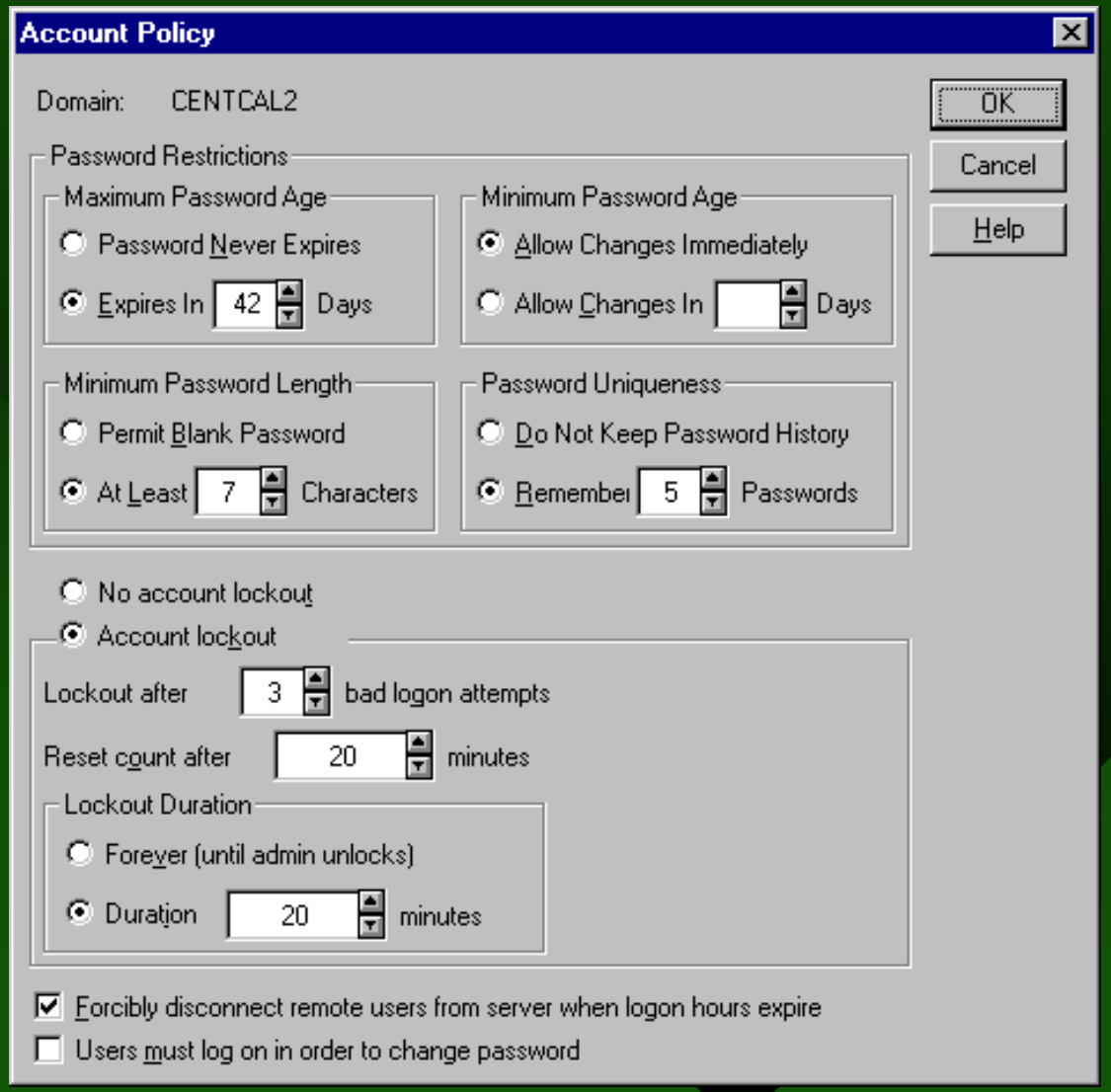
Via rete è possibile intraprendere due tecniche per ottenere la password di Administrator:

- Effettuare una ricerca manuale o automatica
- Intercettare il traffico di autenticazione

Difendersi da i tentativi di ricerca delle password (1)

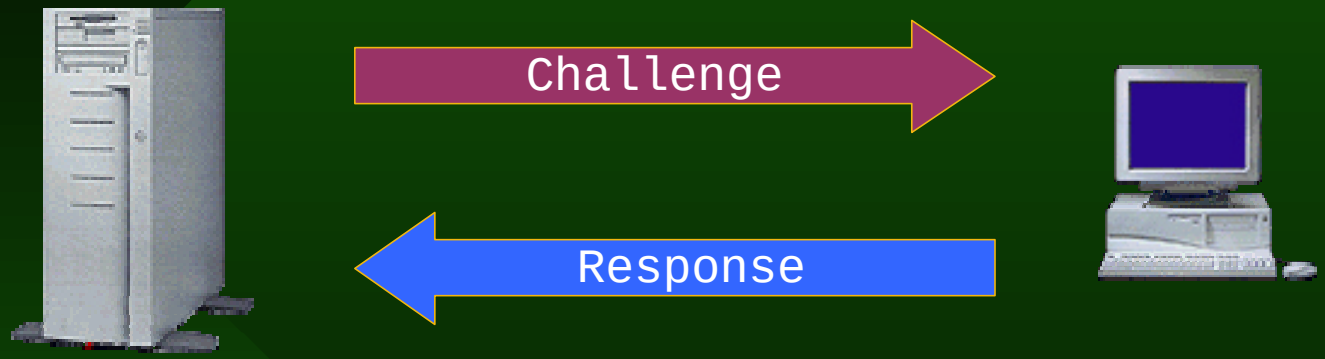
- Installare passfilt (SP2 - Q161990)
- Installare passprop (Resource Kit)
- Filtrare le porte da UDP e TCP da 135 a 137
- Applicare una policy di gestione account
- Limitare gli orari di connessione

Difendersi da i tentativi di ricerca delle password (2)



GARR-CERT
servizio sicurezza GARR

Meccanismo di autenticazione



Algoritmi di cifratura delle password

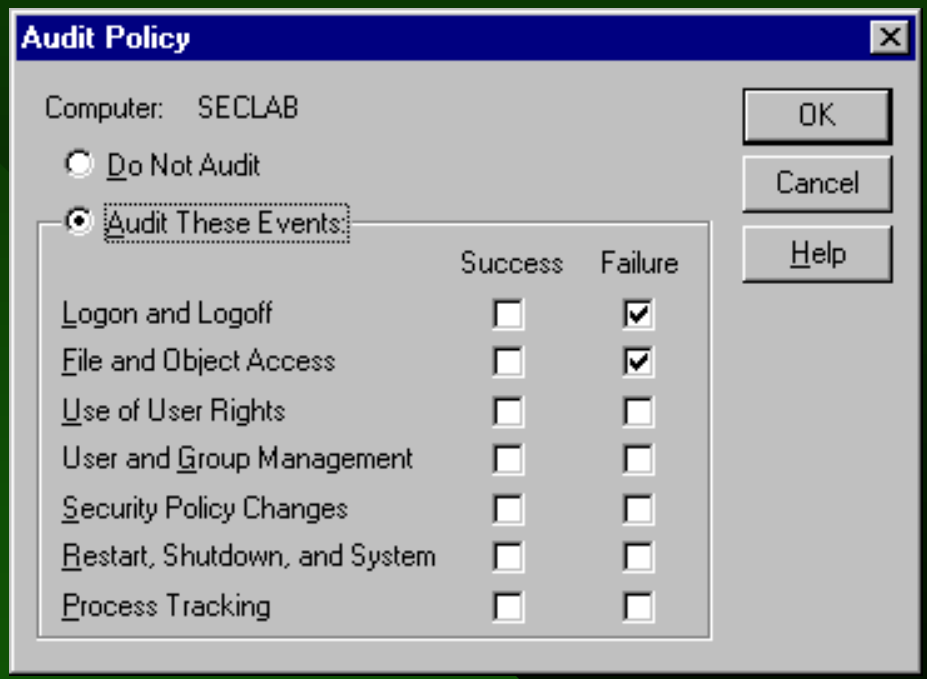
- Hash LanManager
- Hash Windows NT (NTLM e NTLMv2)

Evitare l'intercettazione del traffico di autenticazione (L0phtcrack)

- L'uso di router e switch limita lo sniffing
- Disabilitare l'algoritmo di hash LanManager
  (SP4 - Q147706 - solo per NT)
- Abilitare la "firma" SMB
  (SP3 - Q161372 - solo per NT)

Auditing e Log (1)

Attivare l'auditing per registrare i tentativi di logon falliti



Auditing e Log (2)

Event Viewer - Security Log on \\SECLAB

Log View Options Help

Date	Time	Source	Category	Event	User	Computer
11/15/00	10:05:50 AM	Security	Object Access	560	Administrator	SECLAB
11/13/00	3:25:15 PM	Security	Logon/Logoff	529	SYSTEM	SECLAB
11/13/00	3:25:07 PM	Security	Logon/Logoff	529	SYSTEM	SECLAB
11/13/00	12:07:32 PM	Security	Logon/Logoff	529	SYSTEM	SECLAB
11/13/00	12:07:28 PM	Security	Logon/Logoff	529	SYSTEM	SECLAB
11/13/00	12:07:25 PM	Security	Account Manager	644	SYSTEM	SECLAB
11/13/00	11:54:38 AM	Security	Logon/Logoff	529	SYSTEM	SECLAB
11/13/00	11:54:35 AM	Security	Logon/Logoff	529	SYSTEM	SECLAB
11/13/00	11:54:28 AM	Security	Logon/Logoff	529	SYSTEM	SECLAB
11/13/00	11:54:25 AM	Security	Logon/Logoff	529	SYSTEM	SECLAB
11/13/00	11:51:23 AM	Security	Logon/Logoff	529	SYSTEM	SECLAB
11/13/00	11:51:14 AM	Security	Logon/Logoff	529	SYSTEM	SECLAB
11/13/00	11:51:07 AM	Security	Logon/Logoff	529	SYSTEM	SECLAB
11/10/00	1:47:09 PM	Security	Logon/Logoff	529	SYSTEM	SECLAB
11/10/00	10:56:19 AM	Security	Logon/Logoff	529	SYSTEM	SECLAB
11/10/00	10:56:16 AM	Security	Logon/Logoff	529	SYSTEM	SECLAB
11/10/00	10:52:45 AM	Security	Logon/Logoff	529	SYSTEM	SECLAB
11/10/00	10:52:42 AM	Security	Logon/Logoff	529	SYSTEM	SECLAB
11/10/00	10:27:13 AM	Security	Logon/Logoff	529	SYSTEM	SECLAB
11/10/00	10:23:48 AM	Security	Object Access	560		SECLAB
11/10/00	10:23:48 AM	Security	Object Access	560		SECLAB
11/10/00	10:22:26 AM	Security	Logon/Logoff	529	SYSTEM	SECLAB
11/10/00	10:22:24 AM	Security	Logon/Logoff	529	SYSTEM	SECLAB
11/9/00	4:29:43 PM	Security	Logon/Logoff	529	SYSTEM	SECLAB
11/9/00	4:29:29 PM	Security	Logon/Logoff	529	SYSTEM	SECLAB
11/9/00	4:29:15 PM	Security	Logon/Logoff	529	SYSTEM	SECLAB
11/9/00	4:27:39 PM	Security	Object Access	560		SECLAB
11/9/00	4:27:36 PM	Security	Object Access	560		SECLAB
11/9/00	4:27:36 PM	Security	Object Access	560		SECLAB
11/9/00	4:21:36 PM	Security	Logon/Logoff	529	SYSTEM	SECLAB

Auditing e Log (3)

- Eseguire un'analisi periodica dei log
  - Event Viewer (uso filtri)
  - Dumpel (Resource Kit)
  - Ntlast (versioni free e commerciale)
  - Glaser (versioni free e commerciale)
  - DumpEvt di Somarsoft

IDS e Personal Firewalls

- Sistema dedicato che controlla il traffico in rete
- Software in locale che monitora le trasmisssioni (commerciali)
    - BlackIce Defender
    - ConSeal PC Firewall
    - CyberCop Server

Intrusioni remote tramite exploit

- Buffer overflow remoti
- Denial of Service
  - Pacchetti TCP/IP anomali (applicare SP)
  - Attacco tramite tools DDoS
- Obbiettivo: provocare il reboot del sistema

Ottenere privilegi aggiuntivi (1)

- Rastrellamento delle informazioni

Contromisure:

- Mettersi nei panni dell'hacker
  - srvinfo (Resource Kit)
  - regdmp (Resource Kit)
  - Opzione "Connect Network Registry"

Ottenere privilegi aggiuntivi (2)

- getadmin
  (và avviato in locale e quindi da un operatore)

  contromisura:
  applicare SP3 (Articolo Q146965)

- sechole (secholed)

  contromisura:
  applicare la patch priv-fix (Articolo Q190288)

- Attenzione alla configurazione di IIS

Consolidare il potere ottenuto

Ottenere il SAM `(%systemroot%\system32\config)`

- Boot con un altro sistema operativo
- Copia di backup del SAM creata da RDISK `(%systemroot%\repair)`
- Estrarre direttamente gli hash delle password `(pwdump e pwdump2)`

Crack delle password di NT

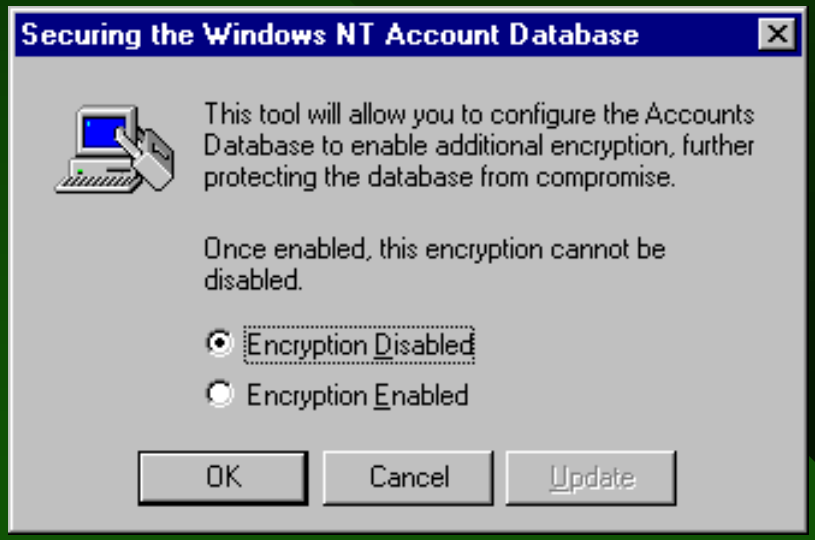
- L0phtcrack
- John the Ripper
- Crack v5

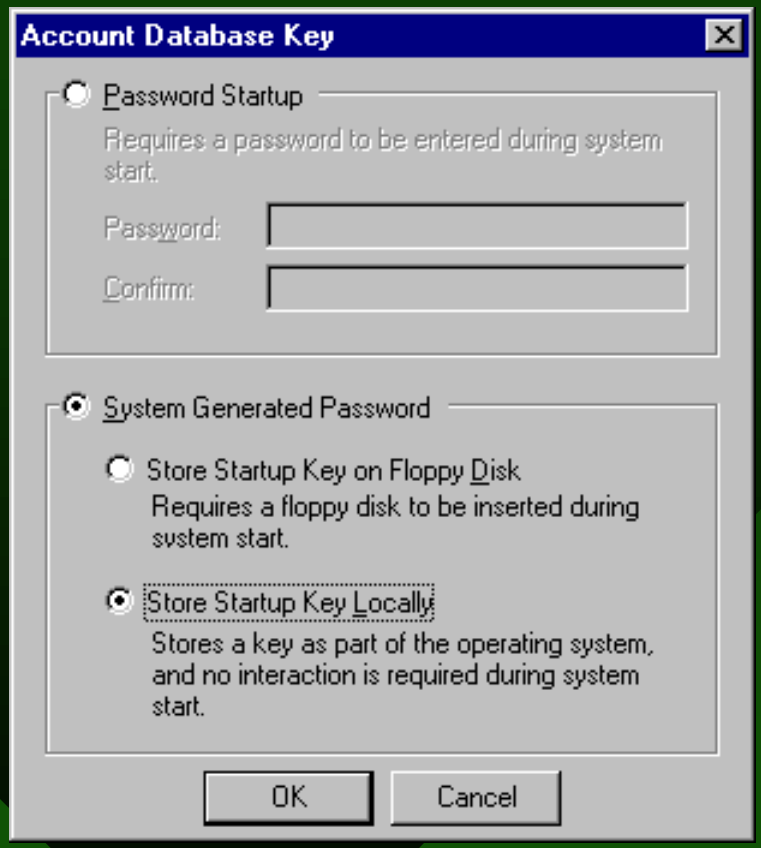
Difese: password robuste

- Lunghezza di 7 o 14 caratteri
- Inserire caratteri ascii non stampabili
  `(almeno per gli amministratori)`

Protezione del SAM

- Applicare SYSKEY (SP2 - Articolo Q143475)





Continuare la ricerca di credenziali di accesso

- Copie locali delle credenziali di Account del dominio (errore frequente, utilizzare su)
- Lettura della chiave LSA Secrets
  `HKEY_LOCAL_MACHINE\SECURITY\Policy\Secretes`

  Contromisure:
  applicare la patch lsa2-fix (Q184017)
  applicare la patch RASPassword-fix (Q230681)

Trojan, Backdoor e Controllo Remoto

- Trojan: Back Orifice, Netbus, listener di netcat ecc.
  (installati tramite exploit o camuffati)
- Controllo Remoto: remote.exe, WinVNC ecc.
- Chiavi del Registry che avviano applicazioni
  (privilegi operatore)

```
HKEY_LOCAL_MACHINE\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\Microsoft\Windows\CurrentVersion\RunOnceEx
HKEY_LOCAL_MACHINE\Microsoft\Windows\CurrentVersion\RunServices
```

- Contromisure: protezione delle chiavi del Registry

```
CREATOR OWNER: Full control
Administrators: Full control
System: Full control
Everyone: Read
```

Copertura delle tracce

- L’hacker disabiliterá l’auditing o cancellará i log
- Contromisure:
  - Creare un sistema di backup centralizzato dei log
  - Utilizzate un software di terze parti

Fonti di informazione

- http://support.microsoft.com
- http://www.microsoft.com/technet/security/current.asp
- http://www.securityfocus.com
- http://www.ntbugtraq.com
- http://www.ntsecurity.net