Protocol Level:

Sicurezza nelle reti Samba

"Vi spaventerò elencandovi alcuni dei problemi delle reti Microsoft"

Diego Fantoma
fantoma@units.it

Dissertazioni preliminari

Questo lavoro non è a carattere tecnico ma è una ricerca bibliografica con alcuni spunti applicativi.

Dopo una lunga esperienza in campo reti, una frase letta per caso può far sorgere un dubbio e inficiare la propria auto considerazione

Scatta allora la curiosità di informarsi e sviscerare gli elementi fondamentali per scoprire se quanto imparato è stato inutile

Il risultato è una raccolta di eccezioni al mio know-how con i ragionamenti - estremamente pratici - che ne sono conseguiti

Protocol Level:

Sicurezza nelle reti Samba

Dal file “LanMan and NT Password Encryption in Samba 2.x” [1]

Important Notes About Security

The unix and SMB password encryption techniques seem similar on the surface. This similarity is, however, only skin deep. The unix scheme typically sends clear text passwords over the network when logging in. This is bad. The SMB encryption scheme never sends the cleartext password over the network but it does store the 16 byte hashed values on disk. This is also bad. Why? Because the 16 byte hashed values are a "password equivalent". You cannot derive the user's password from them, but they could potentially be used in a modified client to gain access to a server. This would require considerable technical knowledge on behalf of the attacker but is perfectly possible. You should thus treat the smbpasswd file as though it contained the cleartext passwords of all your users. Its contents must be kept secret, and the file should be protected accordingly.

Ideally we would like a password scheme which neither requires plain text passwords on the net or on disk. Unfortunately this is not available as Samba is stuck with being compatible with other SMB systems (WinNT, WfWg, Win95 etc).

Warning

Note that Windows NT 4.0 Service pack 3 changed the default for permissible authentication so that plaintext passwords are *never* sent over the wire. The solution to this is either to switch to encrypted passwords with Samba or edit the Windows NT registry to re-enable plaintext passwords. See the document WinNT.txt for details on how to do this.

Other Microsoft operating systems which also exhibit this behavior includes

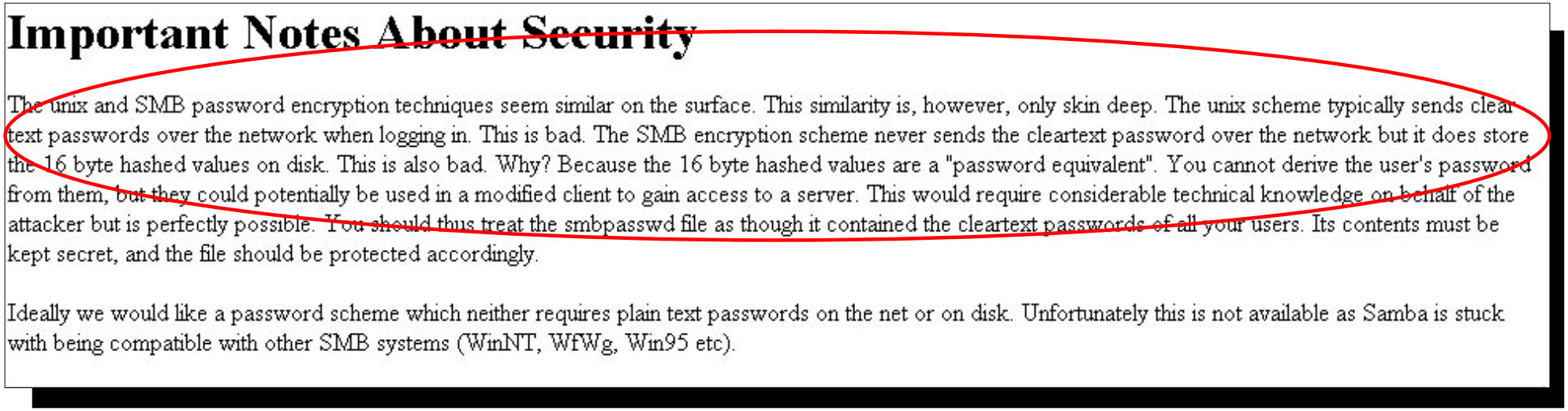
- MS DOS Network client 3.0 with the basic network redirector installed
- Windows 95 with the network redirector update installed
- Windows 98 [se]
- Windows 2000

Note :All current release of Microsoft SMB/CIFS clients support authentication via the SMB Challenge/Response mechanism described here. Enabling clear text authentication does not disable the ability of the client to participate in encrypted authentication.

Diego Fantoma - fantoma@units.it

Protocol Level:

Sicurezza nelle reti Samba



Important Notes About Security

The unix and SMB password encryption techniques seem similar on the surface. This similarity is, however, only skin deep. The unix scheme typically sends clear-text passwords over the network when logging in. This is bad. The SMB encryption scheme never sends the cleartext password over the network but it does store the 16 byte hashed values on disk. This is also bad. Why? Because the 16 byte hashed values are a "password equivalent". You cannot derive the user's password from them, but they could potentially be used in a modified client to gain access to a server. This would require considerable technical knowledge on behalf of the attacker but is perfectly possible. You should thus treat the smbpasswd file as though it contained the cleartext passwords of all your users. Its contents must be kept secret, and the file should be protected accordingly.

Ideally we would like a password scheme which neither requires plain text passwords on the net or on disk. Unfortunately this is not available as Samba is stuck with being compatible with other SMB systems (WinNT, WfWg, Win95 etc).

Lo schema Unix di norma invia sulla rete password in chiaro quando si effettua un login.
Ciò è male.
Lo schema SMB non invia mai password in chiaro sulla rete ma, piuttosto, salva le loro codifiche a 16 bit (Hash) sul disco.
Anche ciò è male.
Perché?
Poiché i valori codificati a 16 bit sono degli equivalenti alle password. Non si possono derivare da questi le password originali degli utenti ma possono venir utilizzati in sistemi modificati per assicurarsi accesso al server.

Diego Fantoma - fantoma@units.it

Protocol Level:

Sicurezza nelle reti Samba

?

CHE FARE ?!?!?

Diego Fantoma - fantoma@units.it

È una questione di probabilità:

E’ più facile che mi sniffino le password nella rete locale

oppure

che riescano ad entrare nel server

?

Diego Fantoma - fantoma@units.it

Sicurezza nelle reti Samba

- La rete locale

L'utilizzo di condivisioni ha senso esclusivamente in reti locali

Talvolta le reti locali si estendono attraverso reti pubbliche (es. tra più sedi, anche molto distanti)

E' indispensabile, in questo caso, l'utilizzo di una VPN

Bisogna configurare Samba affinché accetti connessioni esclusivamente da IP noti

Sicurezza nelle reti Samba

- Minare la sicurezza

Come:

1 da macchine interne alla rete locale, tramite sniffing o da macchine in ascolto su collegamenti esterni, carpendo le password
   - utilizzo degli switches di rete
   - uso una VPN

2 tramite attacco al server
   - devo proteggere il server

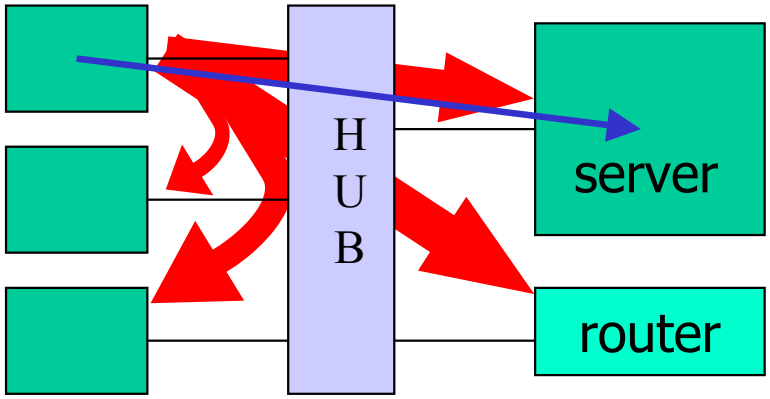
3 tramite attacco ai client
   - devo proteggere i client

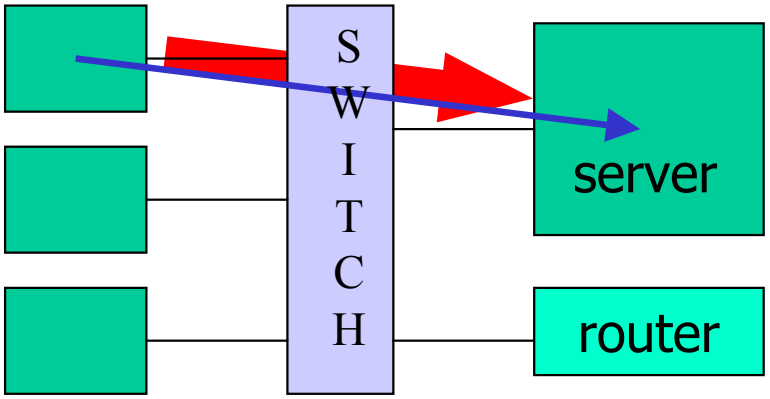
Sicurezza nelle reti Samba

1 - utilizzo di switches e VPN (1/2)

al contrario dei repeater (comunemente chiamati hub) che fanno transitare tutto il traffico in ciascun ramo, gli switches creano dei canali uno-a-uno tra le macchine fra le quali avviene il dialogo.

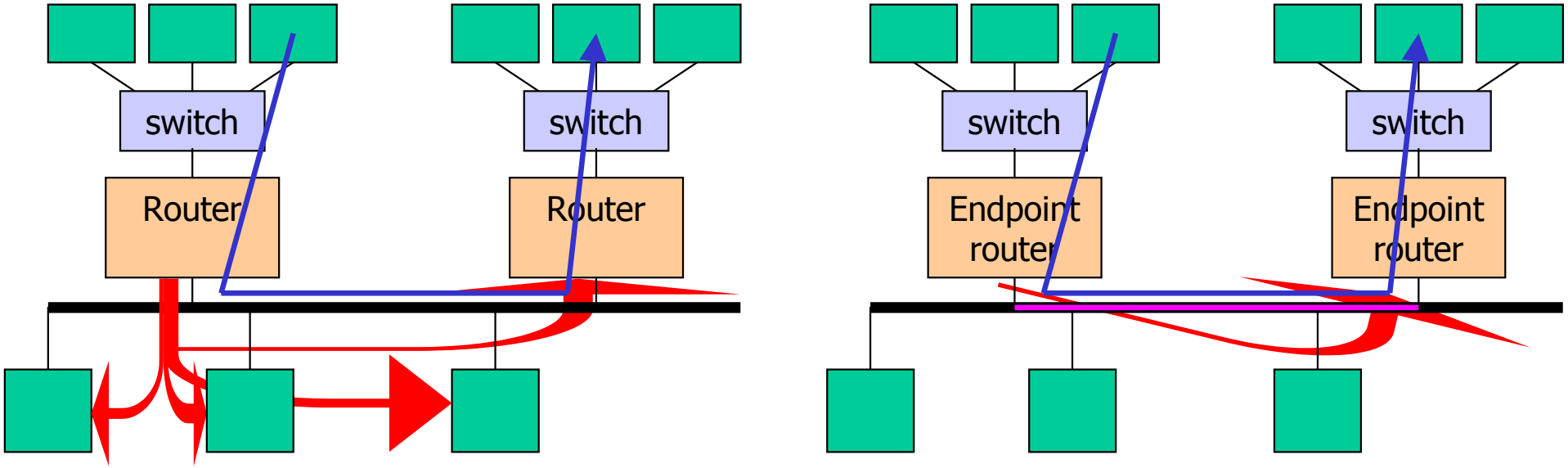
In questo modo evito che vi possano essere delle macchine in ascolto





1 - utilizzo di switches e VPN (2/2)

Su reti pubbliche l'uso di VPN consente una protezione del flusso di pacchetti (criptato) tra due end-point, analogamente a quanto accade con gli switches. Naturalmente il funzionamento è ben diverso ma la canalizzazione ottenuta può esservi assimilata.



2 - Protezione del server (1/8)

Il protocollo CIFS (*Common Internet File System* - RFC1001/1002) adottato da Samba (e Microsoft) sfrutta una serie di porte TCP e UDP sul server che devono essere opportunamente lasciate aperte alle macchine della rete locale e decisamente chiuse ai computer esterni [2]:

```
# cat /etc/services|grep netbios
netbios-ns      137/tcp                         # NETBIOS Name Service
netbios-ns      137/udp                         # NETBIOS Name Service
netbios-dgm     138/tcp                         # NETBIOS Datagram Service
netbios-dgm     138/udp                         # NETBIOS Datagram Service
netbios-ssn     139/tcp                         # NETBIOS Session Service
netbios-ssn     139/udp                         # NETBIOS Session Service
```

2 - Protezione del server (2/8)

Tuttavia bisogna porre attenzione anche ad un altro fenomeno [3]:

Buglet Alert:

The NBT Name Service listens on port 137, but queries may originate from any UDP port number. Such is the nature of UDP. Programs like Samba's `nmblookup` utility will open a high-numbered UDP port (something above 1023) in order to send a query. The reply should be sent back to that same port.

In early versions of Windows 95, however, the source port in `NODE STATUS REQUEST` messages was ignored. The `NODE STATUS RESPONSE` message was sent to UDP port 137--the wrong port. As a result, the node that sent the query might never hear the reply.

Bisogna pertanto tenere conto di questo fattore nel configurare le IPTables:

- Consentire l'uscita del server verso la rete locale qualora venga ricevuta una query, utilizzando il keep state per ricordare la connessione di provenienza

2 - Protezione del server (3/8)

Il file di configurazione di Samba prevede inoltre la possibilità di restringere l'accesso ad una serie di IP e, nel caso in cui il server ne possegga più di una, su determinate interfacce di rete [4]:

```
bind interfaces only = yes
hosts allow = 192.168.100. 127.
interfaces = 192.168.100.101/32
```

2 - Protezione del server (4/8)

Il Name Service può operare in due modalità, eventualmente combinate tra loro.

Nella modalità *broadcast* vengono inviati dei pacchetti UDP broadcast sulla porta 137 con la chiamata ad una macchina e, nel caso in cui il computer chiamato risponda, il suo IP verrà registrato in una tabellina.

Questa modalità è quella normalmente utilizzata nelle reti locali che rimangono all'interno di loro classi di IP: in tal caso bisogna porre attenzione che eventuali filtri, switch o altri apparati non impediscano il broadcast.

Chiaramente, trattandosi di un broadcast IP è da tenere presente che un router, generalmente, non lo lascia transitare.

2 - Protezione del server (5/8)

Nella modalità Point-to-point, invece, a mantenere le tabelline nome-ip è un servizio di rete, NBNS, implementato da Microsoft come WINS.

In tal caso è solamente lui a gestire le richieste di nomenclatura e quindi, non avendo problemi di broadcast, questa soluzione si adatta a situazioni in cui i pacchetti devono venire instradati.

Tuttavia… [5]:

> The problem with the datagram service is that Microsoft messed it up. They made a mistake when they implemented WINS. With the exception of one special case, WINS fails to keep track of IPs associated with a group name. Instead, WINS stores only the generic broadcast address 255. 255.255.255. Because of this, Microsoft never bothered to implement the NBDD. The upshot is that some group members will not receive group multicasts, which has implications for services that rely on group names. We will see an example of this later on when we examine the Browser Service.

2 - Protezione del server (6/8)

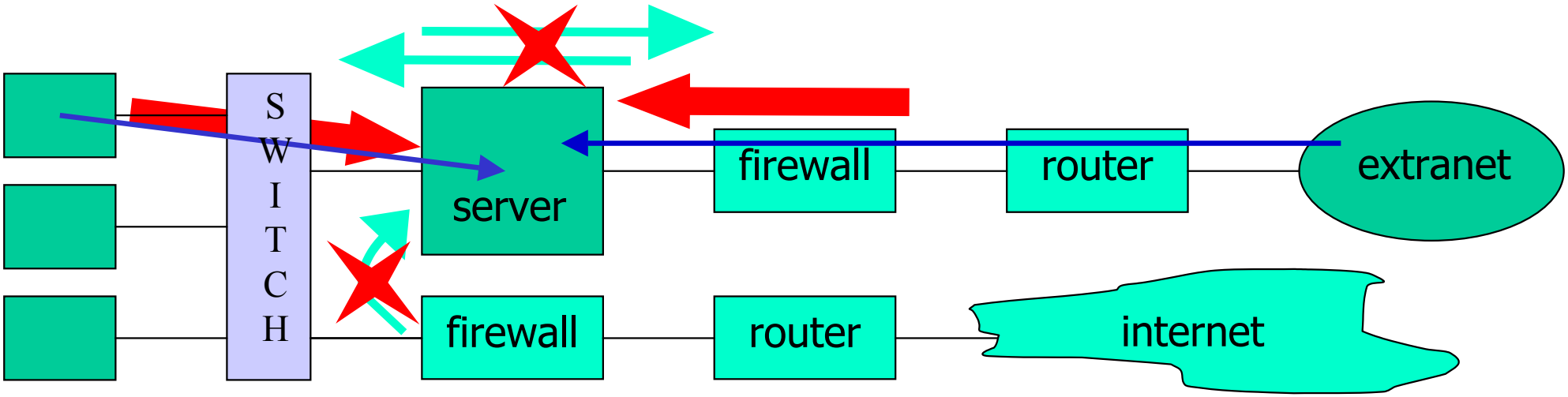
E se non bastasse... [6]:

> Microsoft must have realized their mistake, because they later created what they call "Internet Group" names (also called "Special Group" names). For names in this category, WINS comes close to behaving like a proper NBNS; it will store up to 25 IP addresses per name, deleting the oldest entry to make room if necessary. For these names, a `POSITIVE NAME QUERY RESPONSE` from a WINS server will list up to 25 valid IP addresses.
>
> Internet Group names are identified by their suffix. Originally only group names with the `0x1C` suffix were given special treatment, but more recently (with W2K?) group names with a suffix value of `0x20` can be defined as having Internet Group status. Note that unique names may also have these suffixes but, since they are not group names, no special handling is required.
>
> Sadly, most non-Microsoft implementations (including Samba) follow Microsoft's example. They map group names to the 255.255.255.255 IP address, store only 25 IPs for Special Group names, and fail to implement the NBDD[22]. This can cause trouble for some clients (OS/2, for example) which expect RFC behavior.

Naturalmente il Name Service non è indispensabile al funzionamento della rete - come del resto un DNS - eccezion fatta solamente per i software che lo sfruttano direttamente: è ipotizzabile un mantenimento delle tabelline operato in modo manuale (utilizzando i files LMHOST) e di conseguenza è attuabile la chiusura anche della porta 137.

2 - Protezione del server (7/8)

Inoltre, onde evitare attacchi dall'esterno, è indispensabile proteggere il server con un sistema di firewall che impedisca ingressi non desiderati e, eventualmente, il furto delle hash nel caso in cui utilizzi la crittatura, tenendo conto che in situazioni vincolate a instradamenti si dovrà bene discriminare la extranet dalla internet.



2 - Protezione del server (8/8)

Rimane da chiarire l'utilizzo delle password: criptate o non criptate?

Gli algoritmi di crittatura utilizzati da Linux e dal Challenge/Response sono diversi: è quindi impossibile confrontare direttamente i risultati della ricezione di una password con quelli salvati nel file shadow.

Nonostante esistano svariati tools, nel caso di un server con molti account già attivi, implementare Samba con le password criptate non è da poco conto e, sotto certe condizioni, diventa impossibile effettuare una migrazione. Inoltre ciò significa mantenere una doppia lista utente/password, anche se rende possibile l'uso di due password distinte.

Inoltre bisogna vedere come si comportano eventuali altri server

Considerazioni di massima

Tenuto presente che l'utilizzo di password non criptate mi impone una modifica al registro di configurazione di ciascun client superiore a W95 [*v. slide successiva*], facilmente automatizzabile, si potrebbe dire:

Se ho molti utenti pre esistenti e pochi client (es. aula informatica) conviene adottare le password non criptate;

Se il numero di client è grande e l'inserimento degli utenti deve ancora avvenire, si facilita l'implementazione di password criptate.

Naturalmente le misure di sicurezza dovranno supportare entrambi i sistemi (switch, VPN, firewall) ed essere tenute sempre al massimo dell'efficacia.

Le chiavi del registro di configurazione

Windows 9x

Chiave:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\VxD\VNETSUP
Variabile:	EnablePlainTextPassword
Tipo:	Binario
Per abilitare:	01 00 00 00
Per disabilitare:	00 00 00 00

Windows NT

Chiave:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Rdr\parameters
Variabile:	EnablePlainTextPassword
Tipo:	dword
Per abilitare:	0 0 0 0 0 0 0 1
Per disabilitare:	0 0 0 0 0 0 0 0

Windows 2000, XP

Chiave:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanworkstation\parameters
Variabile:	EnablePlainTextPassword
Tipo:	dword
Per abilitare:	0 0 0 0 0 0 0 1
Per disabilitare:	0 0 0 0 0 0 0 0

3 - Protezione del client (1/3)

Uno dei maggiori problemi di sicurezza è rappresentato dalle macchine che possono usufruire dei servizi, ossia dai client della rete locale.

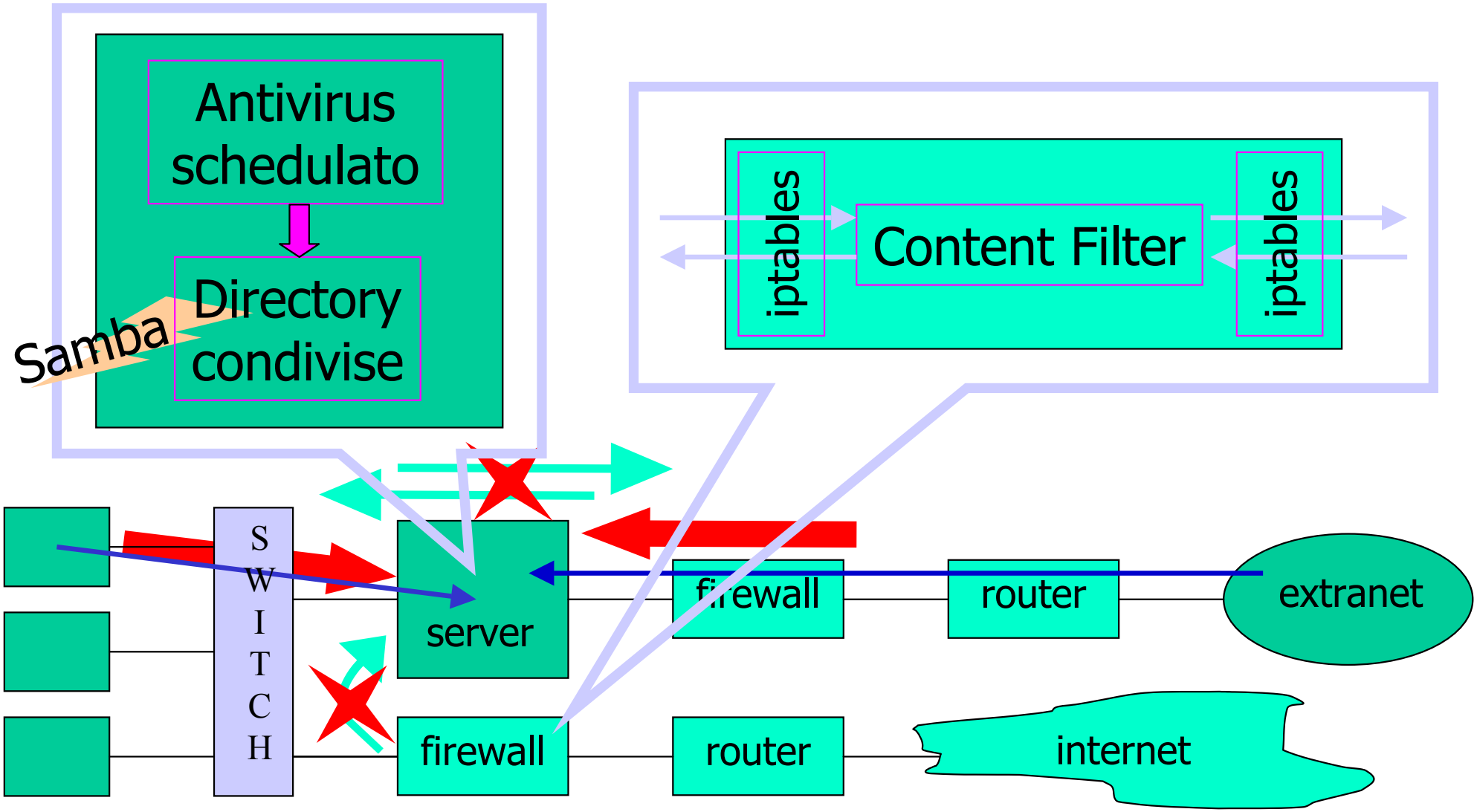
Le macchine possono subire degli attacchi che le rendono a disposizione di altri e diventando fonti di attacco a loro volta nei confronti del server, per esempio iniziando una connessione http come se fosse un browser e poi mettendo a disposizione le risorse delle macchina ad un ipotetico aggressore.

Un'altra forma di attacco sono i virus: Opaserv [8], per esempio, usufruisce delle condivisioni CIFS per infettare altre macchine.

Sono indispensabili quindi un antivirus presente sul server ed un content filter sulle connessioni che intercetti eventuali connessioni del primo tipo.

Sicurezza nelle reti Samba

3 - Protezione del client (2/3)



3 - Protezione del client (3/3)

Chiaramente anche sui client è indispensabile la presenza di un antivirus e di un prodotto che intercetti eventuali software maligni (Application Firewall) controllando che le connessioni in uscita siano provenienti esclusivamente dalle applicazioni concesse (es. l'http solo dal browser).

Un altro problema è la disponibilità, all'interno di una macchina Windows, dei file delle password utente (.pwl), che possono venir carpiti e decodificati in modo da riottenere le password originali [9],[10]:

> Recently, an algorithm was posted on the Internet which can be used to compromise the security used in the password list file. If someone can access the .pwl file on the hard disk of a Windows 95 machine, they may be able to perform operations on the file that can generate the unencrypted password(s).
>
> The Windows 95 password file is only vulnerable when access is available to the .pwl file on the Windows 95 machine's disk.

Conclusioni (1/2)

In questa ricerca bibliografica:

- si sono trattati solo i difetti (alcuni) delle reti CIFS
- si sono viste alcune misure di sicurezza da adottare

Dall'esperienza sappiamo:

- tutti i sistemi e reti hanno punti deboli
- in ogni caso si devono adottare misure di sicurezza
- le misure di sicurezza sono, almeno in parte, comuni

Il mercato:

- è invaso dalle reti CIFS il cui utilizzo è assodato e standard

Conclusioni (2/2)

Reti CIFS:

- Usiamole
- Proteggiamole
- Speriamo bene...

Fonti e riferimenti bibliografici

[1] http://de.samba.org/samba/ftp/docs/htmldocs/ENCRYPTION.html
[2] http://www.linux-mag.com/2001-05/smb_01.html
[3] http://www.ubiqx.org/cifs/
[4] http://de.samba.org/samba/ftp/docs/htmldocs/smb.conf.5.html#BINDINTERFACESONLY
[5] http://www.linux-mag.com/2001-05/smb_04.html
[6] http://www.ubiqx.org/cifs/NetBIOS.html, *1.5.2 - The NBDD and the Damage Done*
[7] http://support.microsoft.com/default.aspx?scid=KB;en-us;q128079
[8] http://www.sophos.com/virusinfo/analyses/w32opaservc.html
[9] http://support.microsoft.com/default.aspx?scid=KB;en-us;q140557
[10] http://support.microsoft.com/default.aspx?scid=kb;EN-US;132807

Computer Programming - Aprile 2002 - "Sicurezza ed affidabilità delle reti eterogenee"
http://online.infomedia.it/riviste/cp/112/articolo13/index.htm