

# Esercitazione 2

## Configurazione di una VPN

Tecnologie e Servizi di Rete

### 1 Introduzione

Scopo dell'esercitazione e' configurare e verificare il funzionamento di una connessione di tipo VPN.

L'esercitazione richiede:

- un PC con un sistema operativo Windows XP SP1 o superiore, accessibile con diritti di amministratore (e' anche possibile utilizzare un diverso sistema operativo ma e' responsabilita' dell'utente documentarsi su come instaurare una connessione VPN con il proprio S.O.)
- un analizzatore di rete installato su PC in uso
- una rete che consenta l'instradamento del protocollo PPTP

### 2 Configurazione della connessione VPN

Lo studente dovra' configurare una VPN con i seguenti parametri:

- server di accesso: 130.192.225.254
- username: `tsr_user`
- password: `sperodiprendereilmassimo`
- autenticazione: Microsoft CHAP
- compressione/cifatura: Nessuna

La configurazione di un adattatore VPN sul sistema Windows XP e' possibile attraverso il link **Create New Connection** dal folder **Network Connections**.

Se non si posseggono i diritti di amministratore, si puo' creare la connessione in questo modo:

**Start -> Programs -> Communication -> New Connection Wizard**

Ricordate di creare uno **shortcut sul desktop** per la nuova connessione, altrimenti sara' impossibile utilizzarla.

Una volta creata la connessione VPN, avviate l'analizzatore di traffico ed instaurate la connessione VPN. Dopodiche' collegatevi con il browser a un sito qualunque (i.e. [www.google.com](http://www.google.com)).

**ATTENZIONE!** Per catturare tutti i protocolli imbustati, bisogna selezionare l'interfaccia fisica, NON l'interfaccia `dialup/VPN`.

## TSR Lab2: Domande e Risposte

1. Indicare il gruppo di appartenenza.

**user\_106**

2. Rappresentare schematicamente un generico pacchetto di traffico (non di inizializzazione) evidenziando gli imbustamenti.

- L'header più esterno è di livello 2, con indirizzo MAC mittente quello della scheda di rete del TEP client ed indirizzo MAC destinazione quello del gateway predefinito (il router casalingo).  
- A seguire troviamo un'intestazione IPv4, i cui indirizzi sono quelli dei due TEP, cioè la macchina client con IP privato 192.168.1.2 (poichè ci si trova dietro NAT con pass-through VPN attivo sul router) e quello del VPN Gateway 130.192.225.254.  
- Dopo abbiamo un'intestazione GRE (identificata da un valore 47 del campo "Protocol Type" dell'intestazione IP), ad indicare che questo è un pacchetto che attraversa il tunnel, il cui campo Protocol indica che l'intestazione successiva è di tipo PPP (valore 0x880b).  
- All'interno di tale intestazione, sempre il campo Protocol, indica un altro header IPv4, stavolta contenente gli indirizzi IP degli host finali, cioè 130.192.225.215 (indirizzo IP interno alla VPN della macchina client da cui ci si connette) e 213.199.181.90 che è l'indirizzo del server di google con cui stiamo instaurando una connessione.  
- A seguire tale intestazione, troviamo quella del segmento TCP, essendo tale pacchetto una richiesta HTTP.  
- Graficamente:

```
- +-----+  
  | MAC | IP(tep) | GRE | PPP | IP(vpn) | TCP | HTTP |  
- +-----+
```

3. Il traffico passa in chiaro o no?

Si, poichè le richieste HTTP sono visibili in chiaro.

4. La fase di autenticazione passa in chiaro o no?

In parte. La password non passa in chiaro, ma il canale non è cifrato.

5. Descrivere brevemente la fase di autenticazione sulla base di quanto osservato nella cattura effettuata

Il sistema operativo utilizzato è windows 7, e per l'autenticazione non si userà CHAP, ma MS-CHAPv2.

Dopo la richiesta di connessione, il PAC (client) ed il PNS (VPN Gateway) si scambiano gli ID di sessione: nel nostro caso abbiamo ID 74 per il client verso il server, 164 per la direzione opposta.

A questo punto il server invia un pacchetto contenente il suo nome (gw2-netgroup) ed una stringa di challenge pseudo-casuale (nonce).

Nel messaggio di risposta il client, oltre ad inviare il suo nome utente (tsr\_user), concatena il suo ID di sessione, la stringa di challenge ricevuta dal VPN gateway e la password (il segreto condiviso), e li cifra tramite DES usando come chiave di cifratura la password stessa.

In ricezione, il VPN gateway esegue lo stesso procedimento e confronta i due risultati.

Se coincidono, il client riceve un messaggio di successo, altrimenti la connessione viene rifiutata e la fase di autenticazione fallisce.

6. Utilizzando Windows XP, configurare le proprietà di TCP/IP per l'adattatore VPN e, nella sezione **Advanced TCP/IP Settings**, disabilitare la checkbox **Use Default Gateway on remote Network**. Eseguire nuovamente la navigazione verso un sito qualunque e indicare i cambiamenti che avvengono con questa diversa impostazione.

- Disabilitando questa opzione, abbiamo reso l'accesso ad internet distribuito e non più centralizzato.

- Ciò vuol dire che i pacchetti diretti verso l'internet pubblico non transitano più attraverso la VPN, e quindi, come mostrano le catture, essi non presentano intestazioni GRE/PPP.

- Pertanto gli indirizzi IP coinvolti sono soltanto quelli finali, cioè quello privato dietro il NAT e quello del server a cui ci si collega.

-

-

-

-

-

-

-

-

-

-

-

-

-

-

-

-

-

-

-