

# CS393 - Network Security - Lab Assignment 6

## Network Defense: IPsec and Snort

### Summary:

In this lab you will learn how to set up VPN tunnels using IPsec. IPsec can be used in several ways and one can set up multiple tunnels to achieve maximum security. In this lab you will explore these properties and set up a tunnel between two hosts in different networks. To do this you will have to cooperate with another team of your choice

### Pre-Lab:

IPSEC is already installed in you machines. To configure it read the documents from the following site:

- [http://www.freeswan.org/freeswan\\_trees/freeswan-1.3/doc/index.html](http://www.freeswan.org/freeswan_trees/freeswan-1.3/doc/index.html)
- <http://www.snort.org/docs/SnortUsersManual.pdf>
- [http://www.snort.org/docs/writing\\_rules/](http://www.snort.org/docs/writing_rules/)

### Part I:

Download, compile and install snort in your team's protected server. Familiarize yourself with snort and its functionalities.

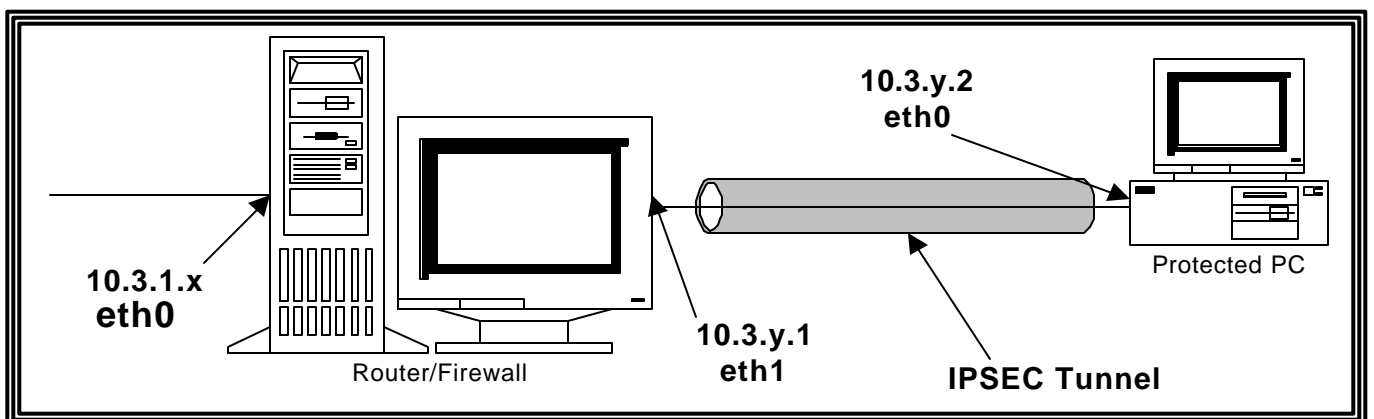
- Use the default rule set supplied in the website and see that it catches the ftp hack, the one you did in the previous lab. (You should perform the hack on your machine). Include the alert message generated in your report

Now develop rules for the following hacks:

- Any packet of size > 100 bytes from network 10.0.0.0 /24 designated to port 80.
- Any packet that contains the following string "Hello CS393"
- Any packet that is designated to a service that is not running in your machine
- Any packet with shell code

Report the above rules in your report with the alert messages generated by snort.

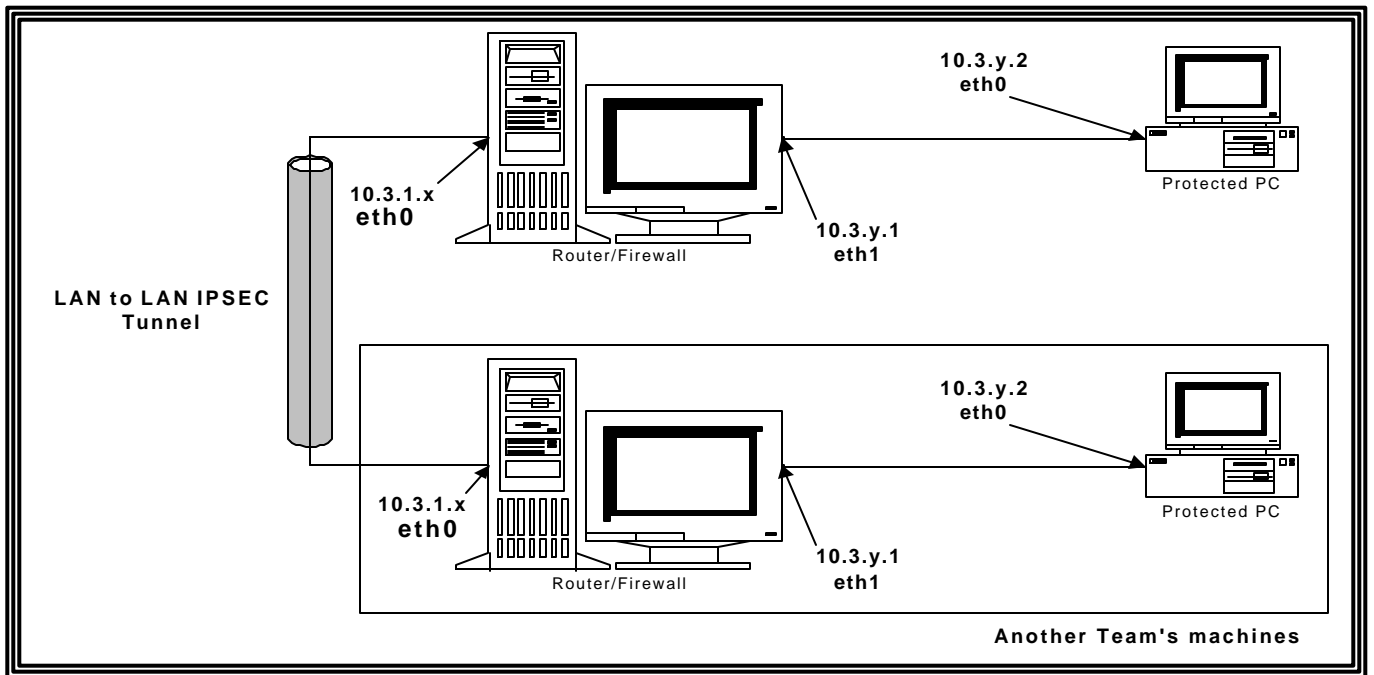
### Part II:



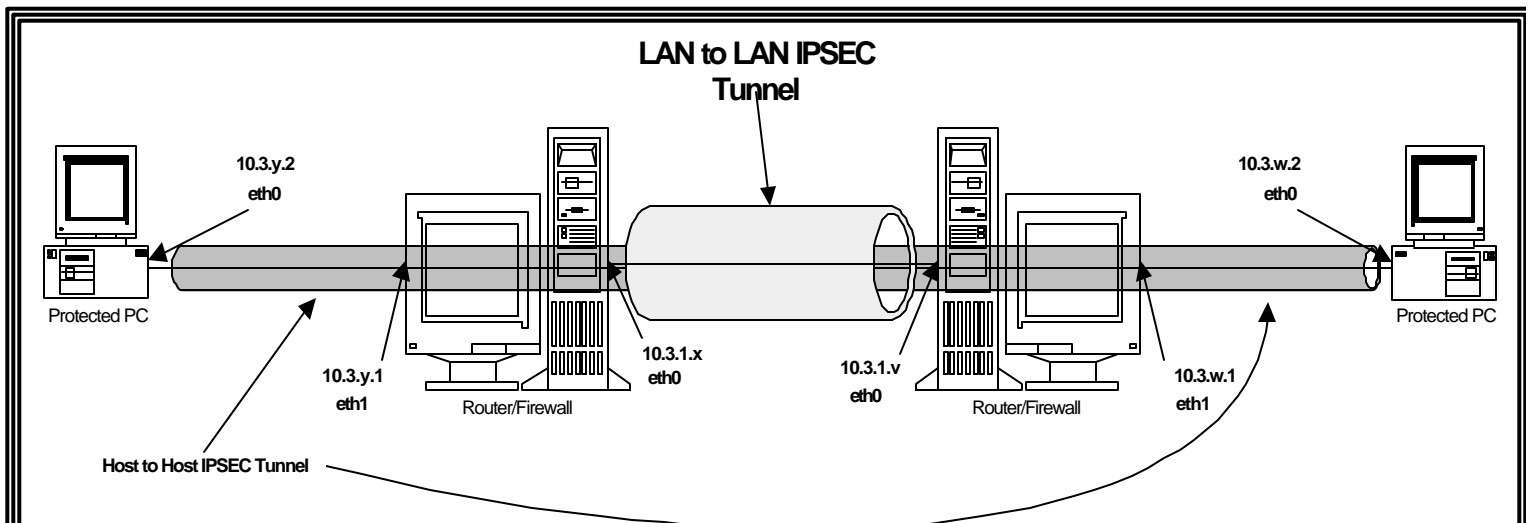
Setup a tunnel between the protected server and your firewall. You must test your tunnel using snort's sniffer and include parts of it to prove that you did infect setup the tunnel. You must also include your configuration file in your report. You are allowed to use secret key authentication instead of RSA

### Part III:

Setup a tunnel between your firewall and another team's firewall. See the figure in the next page. You can use secret key authentication for this part too, which means you'll have to share the keys with the other team. Again you must test your tunnel using snort's sniffer and include parts of it to prove that you did infect setup the tunnel.



### Part IV:



Finally, setup a tunnel between your protected server and the other teams protected server. You can use secret key authentication for this part too, which means you'll have to share the keys with the other team. Again you must test your tunnel using snort's sniffer and include parts of it (sniffed data) to prove that you did setup the tunnel. In your report explain how you did this and must include your configuration file in your report. (ipsec.conf- only the part where you modified)

### **What to hand in?**

- Explain the steps you took to set up Part I
- Explain, in general, how you configured and setup IPSEC tunnels in part II, III and IV. Also include your configuration file in your report. (ipsec.conf- only the part where you modified) you used in each part.