Subject: Re: Firewall rule don't allow ftp while port 21 is open
Posted by Vasily Tarasov on Fri, 06 Oct 2006 07:25:33 GMT
View Forum Message <> Reply to Message

Hello,

Thanks for the script - now we can give it as an example for newbies!
You sad that it doesn't permit ftp access. For me it's wrong: script allows ftp access. Maybe the reason is in a missprint in your script:

```
 # 9) We also would like to allow access to our web server:
      for OURIP in ${SERVER_IPS}; do
        ${FWIN} -p tcp -d ${OURIP} --dport 80 ${OK}
        ${FWIN} -p tcp -d ${OURIP} --dport 443 ${OK}
      done


       10) people are still crazy enough to use ftp                    <<<<  NO SIGN
OF COMMENT (#) IN THE BEGINING!
      for OURIP in ${SERVER_IPS}; do
       for PORT in 20 21; do
        ${FWIN} -p tcp -d ${OURIP} --dport ${PORT} ${OK}
        ${FWIN} -p tcp --sport  ${PORT} -d ${OURIP} --dport 1024: "!" --syn ${OK}
        ${FWIN} -p udp -d ${OURIP} --dport ${PORT} ${OK}
        ${FWIN} -p udp --sport ${PORT} -d ${OURIP} --dport 1024: ${OK}
       done
      done



      # allow answers on high ports
      ${FWIN} -p tcp -m tcp --dport 1024:65535 ! --tcp-flags SYN,RST,ACK SYN ${OK}
      ${FWIN} -p udp -m udp --dport 1024:65535 ${OK}
```

Thanks again!