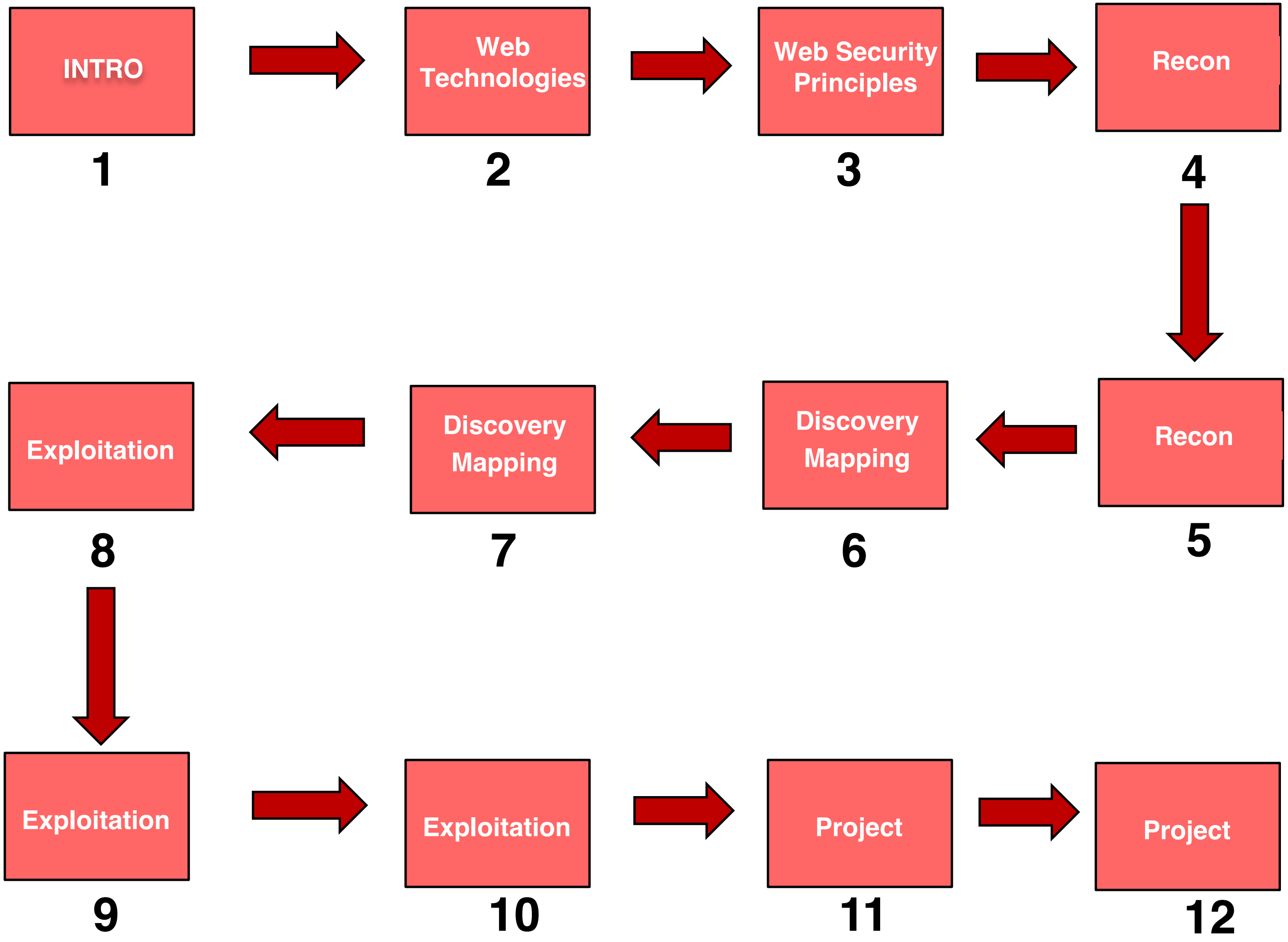
sait.ca
SAIT POLYTECHNIC
FURTHER YOUR PASSION

Web App & Data Base Security

Mapping

Web App & Data Base Security



INTRO
1

Web Technologies
2

Web Security Principles
3

Recon
4

Recon
5

Discovery Mapping
6

Discovery Mapping
7

Exploitation
8

Exploitation
9

Exploitation
10

Project
11

Project
12

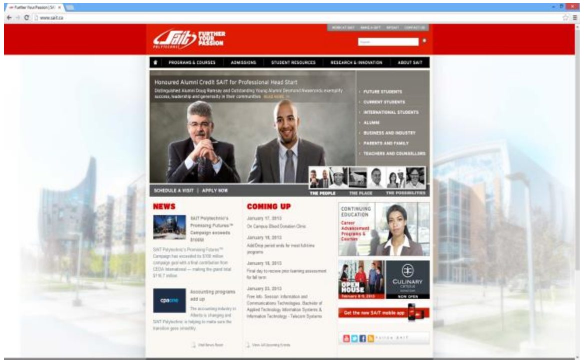
Agenda

- Spidering;
- Robots;
- Proxy Architecture;
- WebScarab;
- Burp Suite;
- Vulnerability Scanning with Nessus.
- Lab 1: Spidering a Website;
- Lab 2: Discovering Vulnerabilities on web services.

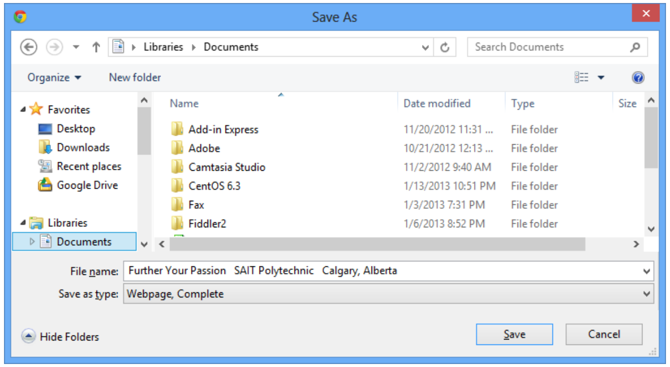
Spidering the Target Web Site

Mapping

- This is next step of mapping phase, spidering a web site;
- It involves following web links to download a copy of an entire site;
- It's used to analyze a web site offline;
- Also known as crawling a web site;
- Browsing the web site and save each page.



Save as →



Name	Date modified	Type	Size
Add-in Express	11/20/2012 11:31 ...	File folder	
Adobe	10/21/2012 12:13 ...	File folder	
Camtasia Studio	11/2/2012 9:40 AM	File folder	
CentOS 6.3	1/13/2013 10:51 PM	File folder	
Fax	1/3/2013 7:31 PM	File folder	
Fiddler2	1/6/2013 8:52 PM	File folder	

File name: Further Your Passion SAIT Polytechnic Calgary, Alberta

Save as type: Webpage, Complete

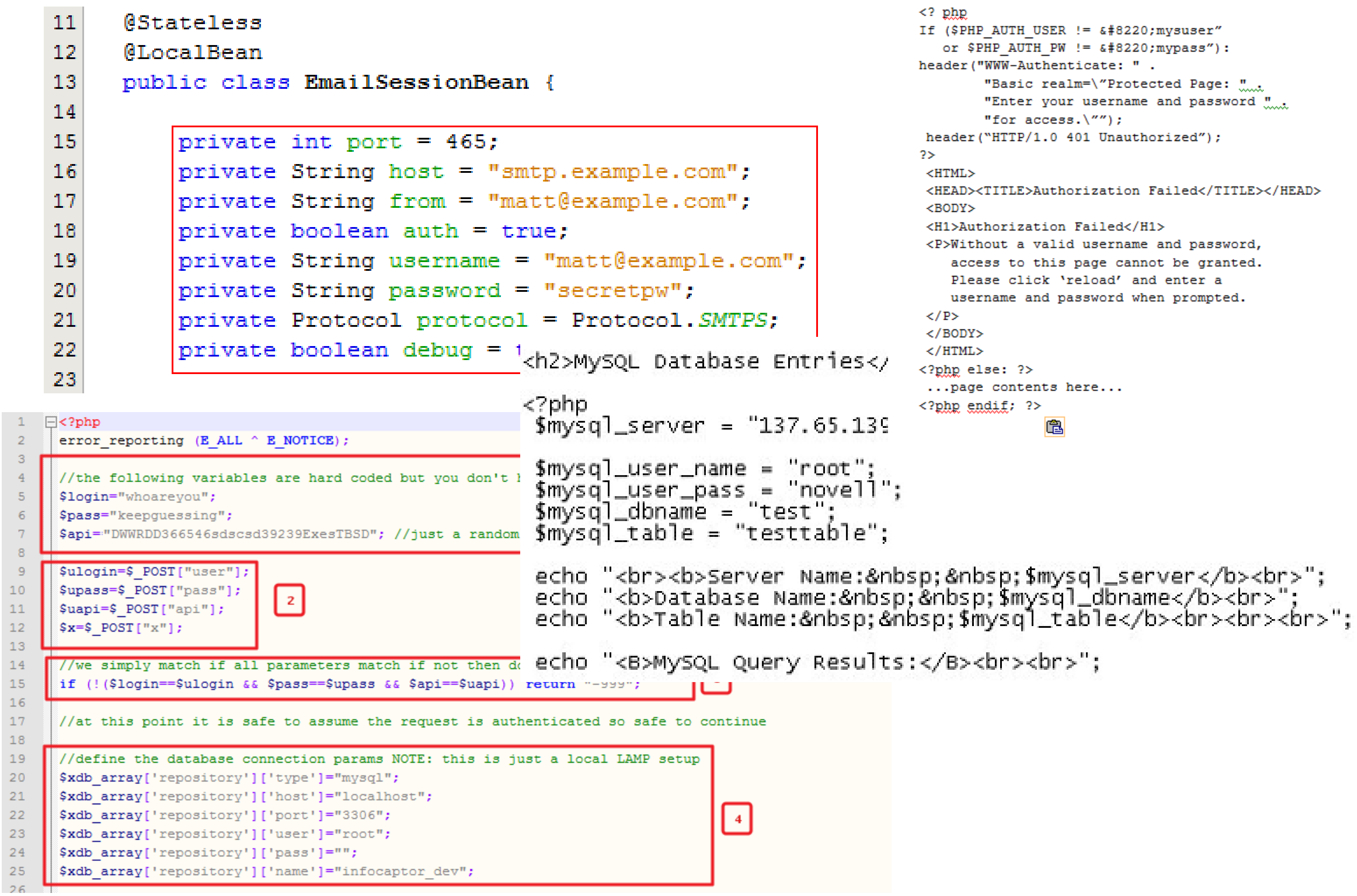
Spidering the Target Web Site

What to look for during the spidering exercise:

- Links, web forms, directories;
- Find security weaknesses in code;
- Email addresses, names, phone numbers;
- Comments that reveal useful or sensitive information;
- Commented code and links;
- Disabled functionality;
- Passwords, user information hard coded.

Spidering the Target Web Site

Mapping



```java
@Stateless
@LocalBean
public class EmailSessionBean {

        private int port = 465;
        private String host = "smtp.example.com";
        private String from = "matt@example.com";
        private boolean auth = true;
        private String username = "matt@example.com";
        private String password = "secretpw";
        private Protocol protocol = Protocol.SMTPS;
        private boolean debug = t
```

```php
<?php
error_reporting (E_ALL ^ E_NOTICE);

//the following variables are hard coded but you don't 
$login="whoareyou";
$pass="keepguessing";
$api="DWWRDD366546sdscsd39239ExesTBSD"; //just a random

$ulogin=$_POST["user"];
$upass=$_POST["pass"];
$uapi=$_POST["api"];
$x=$_POST["x"];

//we simply match if all parameters match if not then do
if (!($login==$ulogin && $pass==$upass && $api==$uapi)) return "-999";

//at this point it is safe to assume the request is authenticated so safe to continue

//define the database connection params NOTE: this is just a local LAMP setup
$xdb_array['repository']['type']="mysql";
$xdb_array['repository']['host']="localhost";
$xdb_array['repository']['port']="3306";
$xdb_array['repository']['user']="root";
$xdb_array['repository']['pass']="";
$xdb_array['repository']['name']="infocaptor_dev";
```

```php
<h2>MySQL Database Entries</

<?php
 $mysql_server = "137.65.139

 $mysql_user_name = "root";
 $mysql_user_pass = "novell";
 $mysql_dbname = "test";
 $mysql_table = "testtable";

 echo "<br><b>Server Name:&nbsp;&nbsp;$mysql_server</b><br>";
 echo "<b>Database Name:&nbsp;&nbsp;$mysql_dbname</b><br>";
 echo "<b>Table Name:&nbsp;&nbsp;$mysql_table</b><br><br><br>";

 echo "<B>MySQL Query Results:</B><br><br>";
```

```php
<? php
If ($PHP_AUTH_USER != &#8220;mysuser”
   or $PHP_AUTH_PW != &#8220;mypass”):
header("WWW-Authenticate: " .
        "Basic realm=\”Protected Page: " .
        "Enter your username and password " .
        "for access.\””);
 header(“HTTP/1.0 401 Unauthorized”);
?>
 <HTML>
 <HEAD><TITLE>Authorization Failed</TITLE></HEAD>
 <BODY>
 <H1>Authorization Failed</H1>
 <P>Without a valid username and password,
    access to this page cannot be granted.
    Please click ‘reload’ and enter a
    username and password when prompted.
 </P>
 </BODY>
 </HTML>
<?php else: ?>
 ...page contents here...
<?php endif; ?>
```

Spidering Methods

- Manual and automated spidering;
- Manual browsing the site and save each page;
- May be necessary if automated scanning fails;
- Automated scans may fail because the site is complex or has issues;
- Automated tools:
  - Wget;
  - WebScarab;
  - Burp Suite;
  - Paros.

Robot Control – Robot.txt

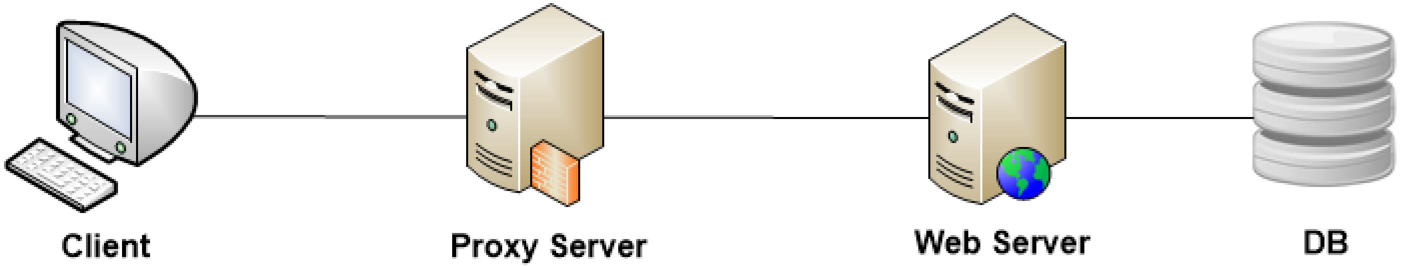
Mapping

- Automated spidering tools are commonly referred to as robot or bots;
- One method of controlling this type of robot is robots.txt file:
    - It’s placed in the document root of the web app, readable by anyone accessing the website;
    - Specifies which user-agent types should be disallowed access to certain directories or individual pages;
    - Contains a list of URLs that the site does not want web spiders to visit or search engines to index;
    - This files contains references to sensitive functionality, which it’s certainly interested in spidering.

Mapping

Proxy Servers Architecture

- A proxy server front ends for one or more application (called reverse proxy);
- The proxy passed requests thru the application and caches the results;
- Adds one more layer of protection.



WebScarab

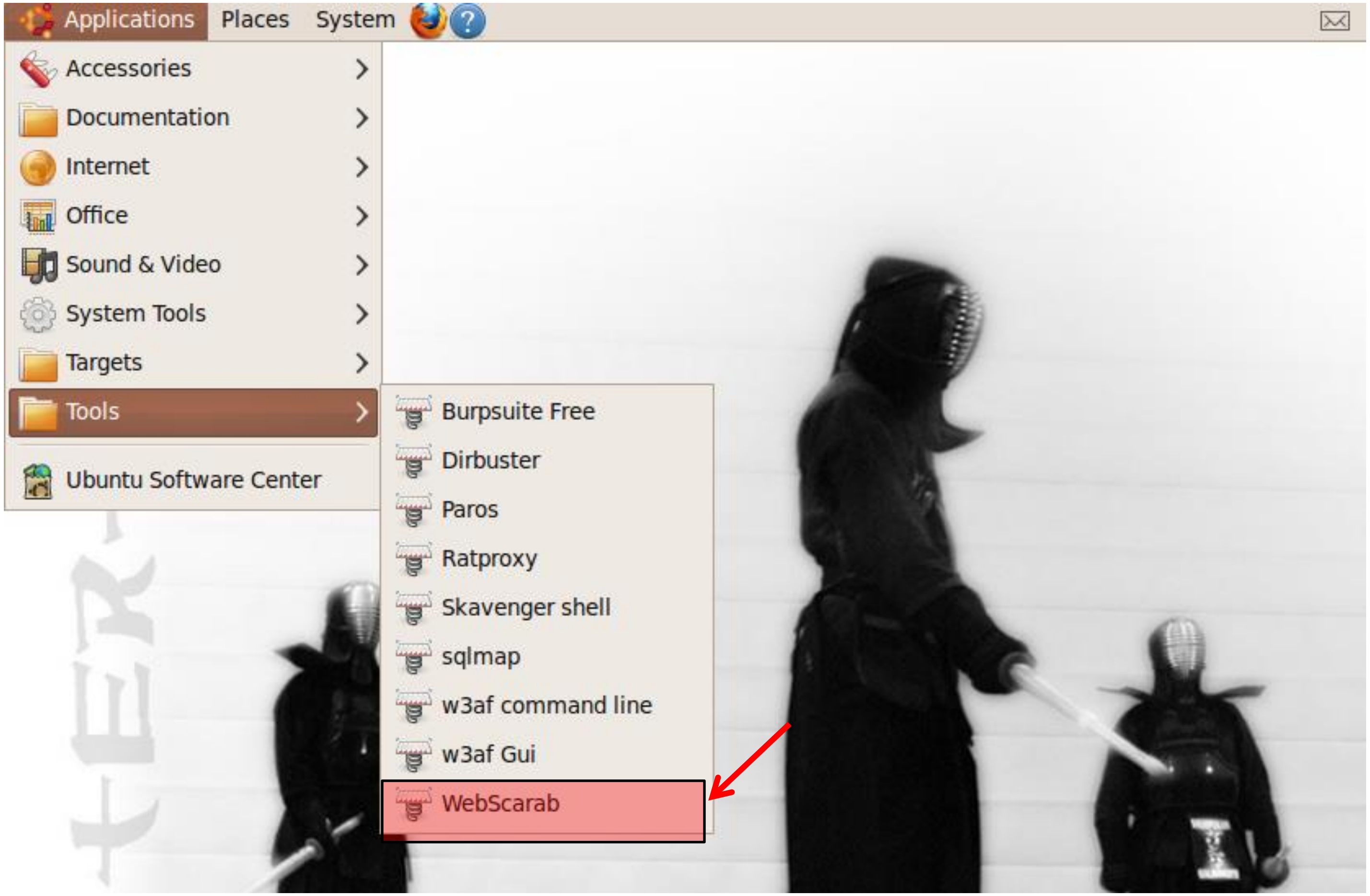
- It operates as an intercepting proxy from OWASP;
- Observes traffic between the browser and the web server;
- Spidering is primed by using the interception proxy;
- WebScarab is a framework for analyzing applications that communicate using the HTTP and HTTPS protocols;
- It is written in Java, and is thus portable to many platforms;
- Allows the operator to review and modify requests created by the browser before they are sent to the server;

  Review and modify responses returned from the server before they are received by the browser.

Spidering a Website - WebScarab

Mapping

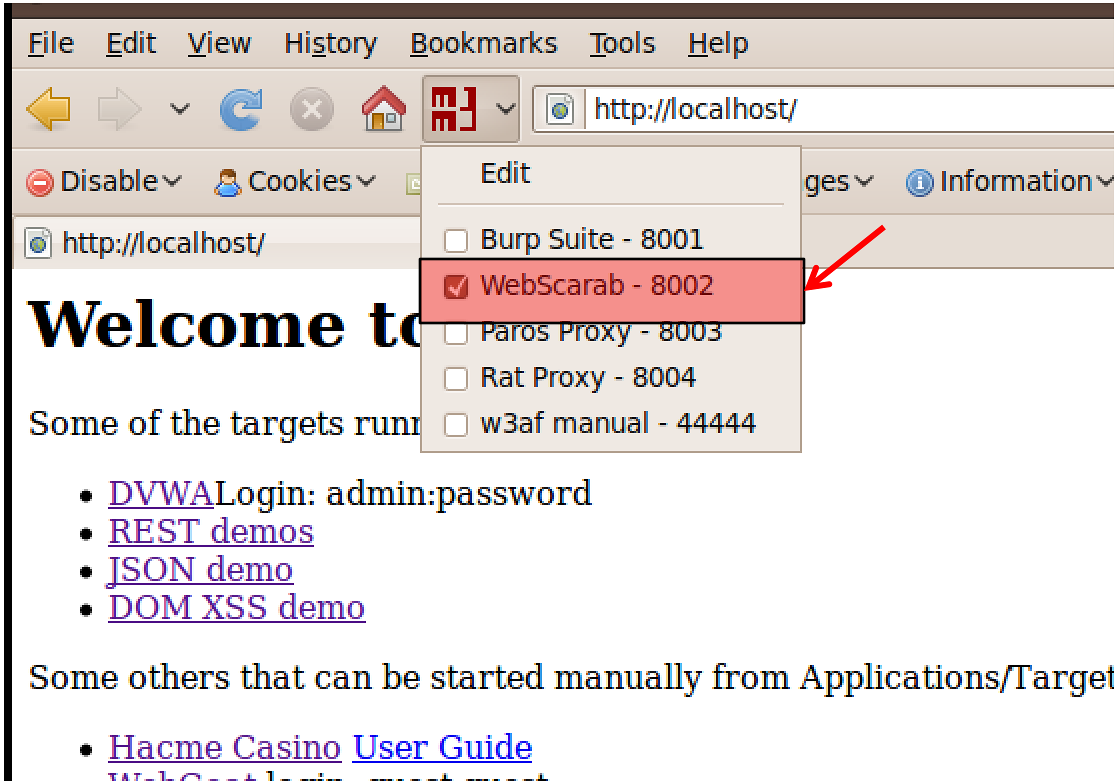
Step 1: Starting the intercepting proxy



Spidering a Website - WebScarab

Mapping

Step 2: Selecting the proxy – WebScarab:8002



□ Burp Suite - 8001
☑ WebScarab - 8002
□ Paros Proxy - 8003
□ Rat Proxy - 8004
□ w3af manual - 44444

Welcome t

Some of the targets runn

- DVWALogin: admin:password
- REST demos
- JSON demo
- DOM XSS demo

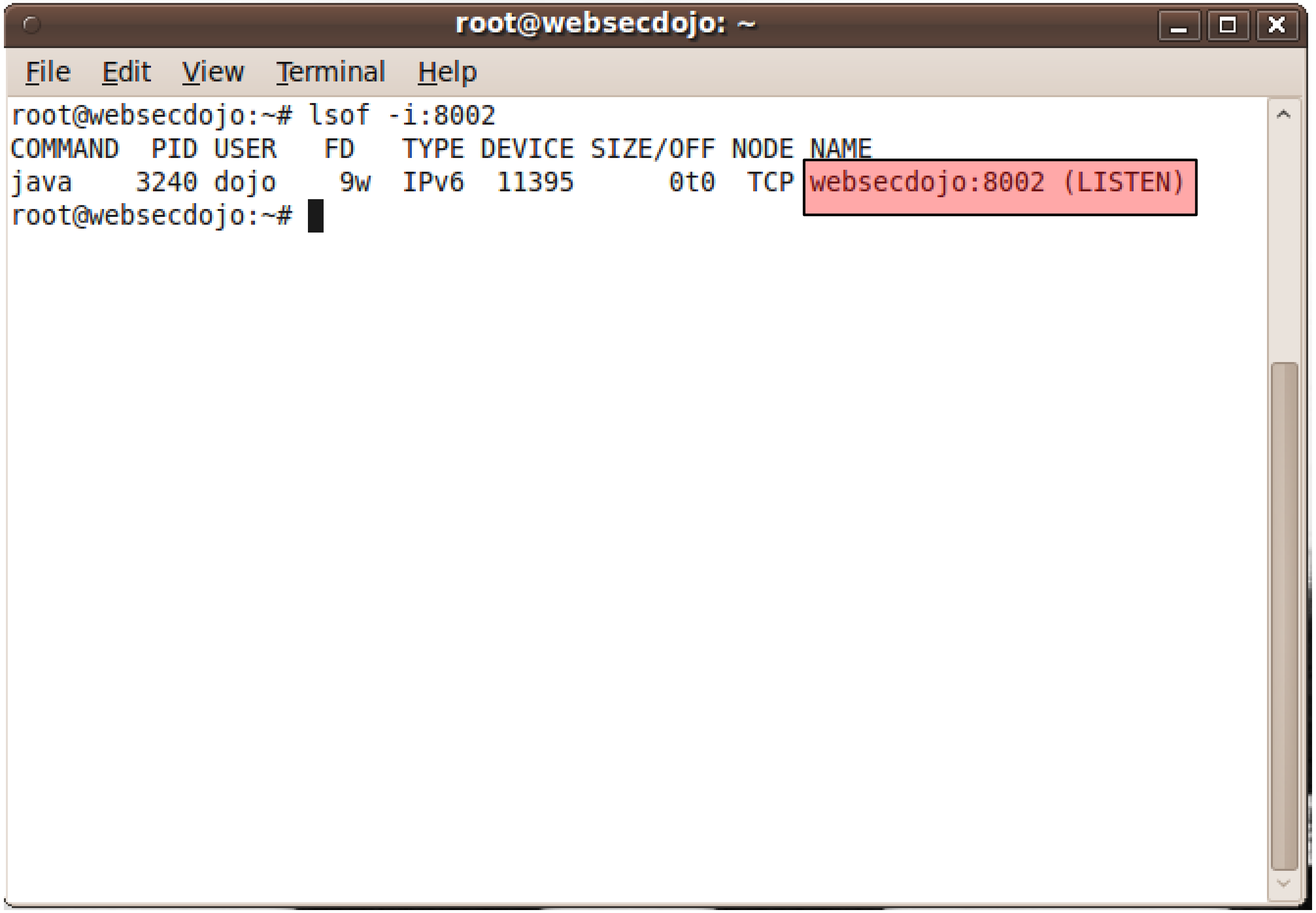
Some others that can be started manually from Applications/Target

- Hacme Casino User Guide

Spidering a Website - WebScarab

Mapping

Step 2: Selecting the proxy – WebScarab:8002

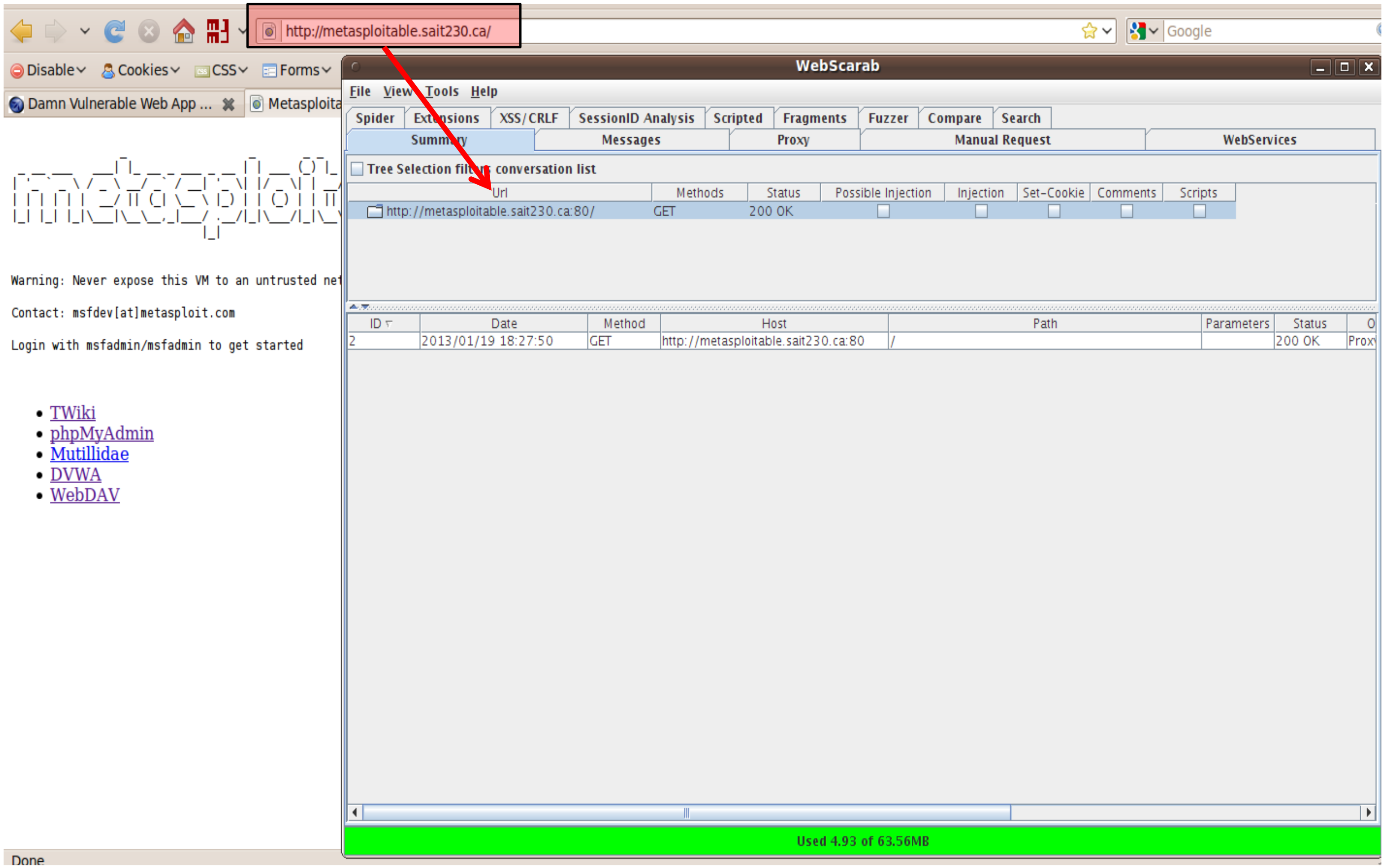


```
root@websecdojo:~# lsof -i:8002
COMMAND   PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
java     3240 dojo    9w  IPv6  11395      0t0  TCP websecdojo:8002 (LISTEN)
root@websecdojo:~# 
```

Spidering a Website - WebScarab

Mapping

Step 3: Browsing the target web app



http://metasploitable.sait230.ca/

```
Warning: Never expose this VM to an untrusted net

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

☐ Tree Selection filters conversation list

Url	Methods	Status	Possible Injection	Injection	Set-Cookie	Comments	Scripts
http://metasploitable.sait230.ca:80/	GET	200 OK	☐	☐	☐	☐	☐

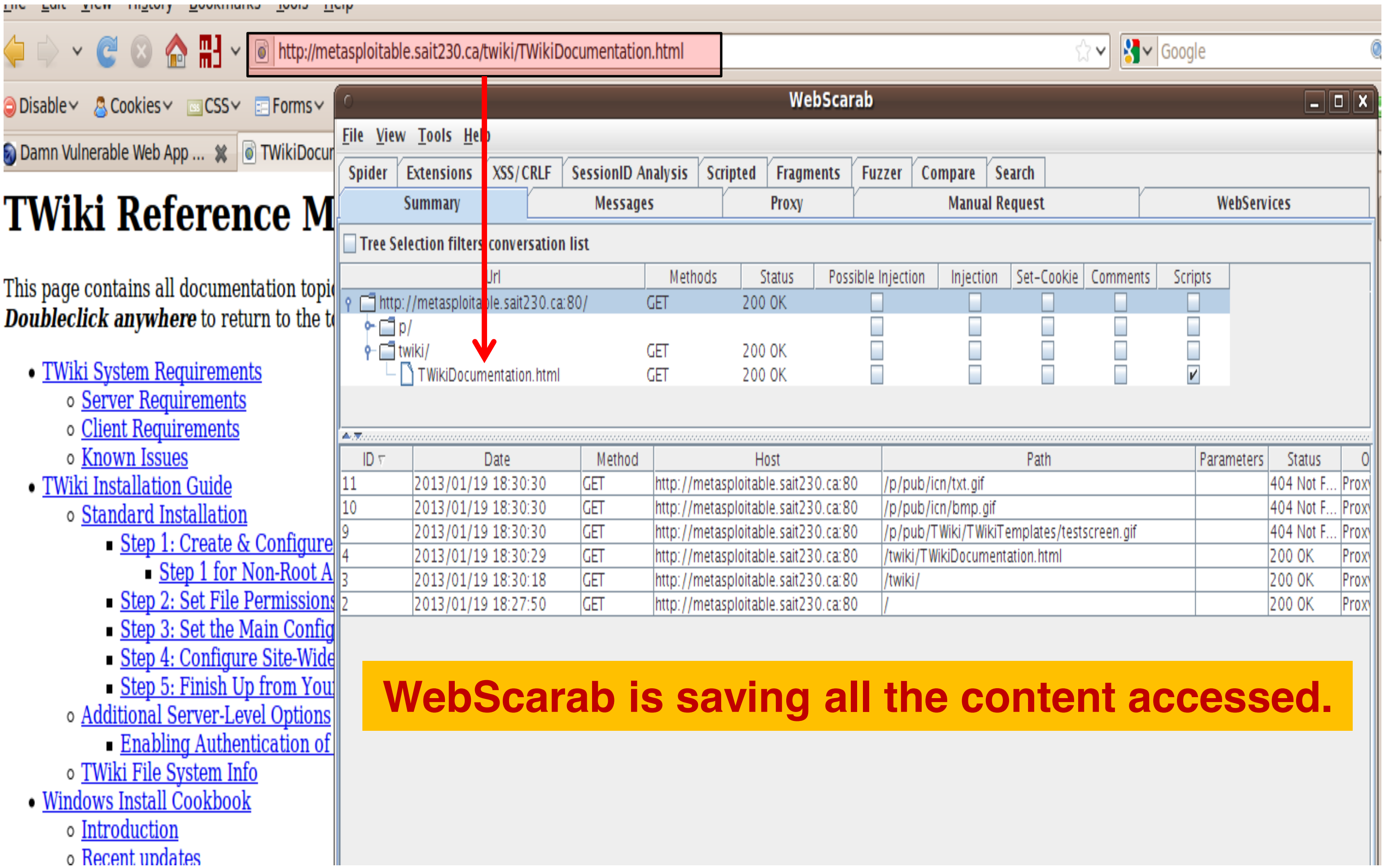
ID	Date	Method	Host	Path	Parameters	Status	O
2	2013/01/19 18:27:50	GET	http://metasploitable.sait230.ca:80	/		200 OK	Prox

Used 4.93 of 63.56MB

Spidering a Website - WebScarab

Mapping

Step 3: Browsing the target web app



File Edit View History Bookmarks Tools Help

http://metasploitable.sait230.ca/twiki/TWikiDocumentation.html

Google
Disable Cookies CSS Forms
Damn Vulnerable Web App ...
TWikiDocur

TWiki Reference M

This page contains all documentation topi
Doubleclick anywhere to return to the t

- TWiki System Requirements
  - Server Requirements
  - Client Requirements
  - Known Issues
- TWiki Installation Guide
  - Standard Installation
    - Step 1: Create & Configure
      - Step 1 for Non-Root A
    - Step 2: Set File Permissions
    - Step 3: Set the Main Config
    - Step 4: Configure Site-Wide
    - Step 5: Finish Up from You
  - Additional Server-Level Options
    - Enabling Authentication of
  - TWiki File System Info
- Windows Install Cookbook
  - Introduction
  - Recent updates

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://metasploitable.sait230.ca:80/	GET	200 OK	□	□	□	□	□
p/			□	□	□	□	□
twiki/	GET	200 OK	□	□	□	□	□
TWikiDocumentation.html	GET	200 OK	□	□	□	□	☑

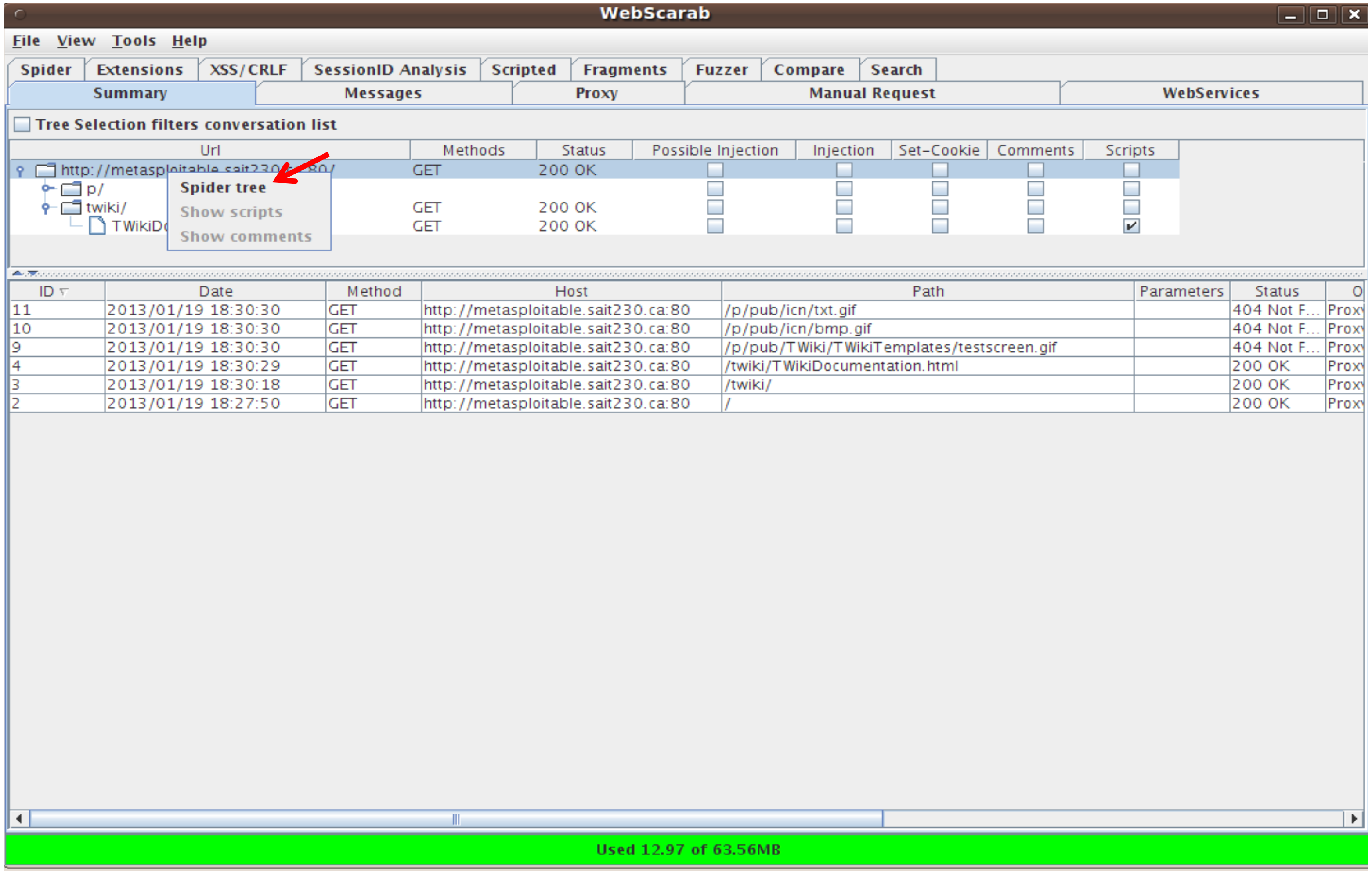
ID	Date	Method	Host	Path	Parameters	Status	O
11	2013/01/19 18:30:30	GET	http://metasploitable.sait230.ca:80	/p/pub/icn/txt.gif		404 Not F...	Prox
10	2013/01/19 18:30:30	GET	http://metasploitable.sait230.ca:80	/p/pub/icn/bmp.gif		404 Not F...	Prox
9	2013/01/19 18:30:30	GET	http://metasploitable.sait230.ca:80	/p/pub/TWiki/TWikiTemplates/testscreen.gif		404 Not F...	Prox
4	2013/01/19 18:30:29	GET	http://metasploitable.sait230.ca:80	/twiki/TWikiDocumentation.html		200 OK	Prox
3	2013/01/19 18:30:18	GET	http://metasploitable.sait230.ca:80	/twiki/		200 OK	Prox
2	2013/01/19 18:27:50	GET	http://metasploitable.sait230.ca:80	/		200 OK	Prox

WebScarab is saving all the content accessed.

Spidering a Website - WebScarab

Mapping

Step 4: WebScarab Console - Summary



□ Tree Selection filters conversation list

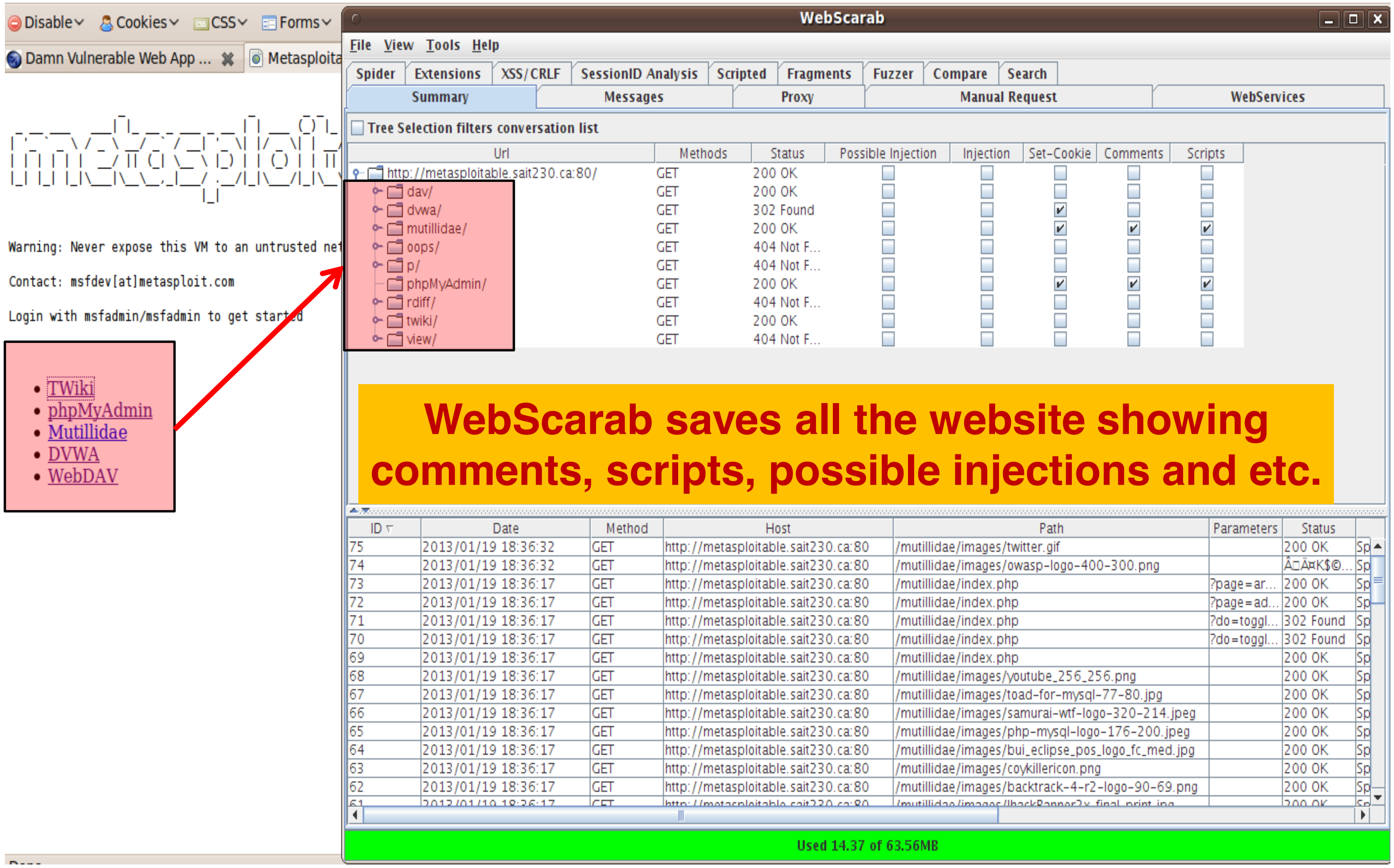
Url	Methods	Status	Possible Injection	Injection	Set-Cookie	Comments	Scripts
http://metasploitable.sait230.ca:80/	GET	200 OK	□	□	□	□	□
p/			□	□	□	□	□
twiki/	GET	200 OK	□	□	□	□	□
TWikiD	GET	200 OK	□	□	□	□	☑

ID	Date	Method	Host	Path	Parameters	Status	O
11	2013/01/19 18:30:30	GET	http://metasploitable.sait230.ca:80	/p/pub/icn/txt.gif		404 Not F...	Prox
10	2013/01/19 18:30:30	GET	http://metasploitable.sait230.ca:80	/p/pub/icn/bmp.gif		404 Not F...	Prox
9	2013/01/19 18:30:30	GET	http://metasploitable.sait230.ca:80	/p/pub/TWiki/TWikiTemplates/testscreen.gif		404 Not F...	Prox
4	2013/01/19 18:30:29	GET	http://metasploitable.sait230.ca:80	/twiki/TWikiDocumentation.html		200 OK	Prox
3	2013/01/19 18:30:18	GET	http://metasploitable.sait230.ca:80	/twiki/		200 OK	Prox
2	2013/01/19 18:27:50	GET	http://metasploitable.sait230.ca:80	/		200 OK	Prox

Mapping

Spidering a Website - WebScarab

Step 4: WebScarab Console - Summary



Warning: Never expose this VM to an untrusted net

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

□ Tree Selection filters conversation list

Url	Methods	Status	Possible Injection	Injection	Set-Cookie	Comments	Scripts
http://metasploitable.sait230.ca:80/	GET	200 OK	□	□	□	□	□
dav/	GET	200 OK	□	□	□	□	□
dvwa/	GET	302 Found	□	□	☑	□	□
mutillidae/	GET	200 OK	□	□	☑	☑	☑
oops/	GET	404 Not F...	□	□	□	□	□
p/	GET	404 Not F...	□	□	□	□	□
phpMyAdmin/	GET	200 OK	□	□	☑	☑	☑
rdiff/	GET	404 Not F...	□	□	□	□	□
twiki/	GET	200 OK	□	□	□	□	□
view/	GET	404 Not F...	□	□	□	□	□

WebScarab saves all the website showing comments, scripts, possible injections and etc.

ID	Date	Method	Host	Path	Parameters	Status	
75	2013/01/19 18:36:32	GET	http://metasploitable.sait230.ca:80	/mutillidae/images/twitter.gif		200 OK	Sp
74	2013/01/19 18:36:32	GET	http://metasploitable.sait230.ca:80	/mutillidae/images/owasp-logo-400-300.png		Â□Ä¤K$©...	Sp
73	2013/01/19 18:36:17	GET	http://metasploitable.sait230.ca:80	/mutillidae/index.php	?page=ar...	200 OK	Sp
72	2013/01/19 18:36:17	GET	http://metasploitable.sait230.ca:80	/mutillidae/index.php	?page=ad...	200 OK	Sp
71	2013/01/19 18:36:17	GET	http://metasploitable.sait230.ca:80	/mutillidae/index.php	?do=toggl...	302 Found	Sp
70	2013/01/19 18:36:17	GET	http://metasploitable.sait230.ca:80	/mutillidae/index.php	?do=toggl...	302 Found	Sp
69	2013/01/19 18:36:17	GET	http://metasploitable.sait230.ca:80	/mutillidae/index.php		200 OK	Sp
68	2013/01/19 18:36:17	GET	http://metasploitable.sait230.ca:80	/mutillidae/images/youtube_256_256.png		200 OK	Sp
67	2013/01/19 18:36:17	GET	http://metasploitable.sait230.ca:80	/mutillidae/images/toad-for-mysql-77-80.jpg		200 OK	Sp
66	2013/01/19 18:36:17	GET	http://metasploitable.sait230.ca:80	/mutillidae/images/samurai-wtf-logo-320-214.jpeg		200 OK	Sp
65	2013/01/19 18:36:17	GET	http://metasploitable.sait230.ca:80	/mutillidae/images/php-mysql-logo-176-200.jpeg		200 OK	Sp
64	2013/01/19 18:36:17	GET	http://metasploitable.sait230.ca:80	/mutillidae/images/bui_eclipse_pos_logo_fc_med.jpg		200 OK	Sp
63	2013/01/19 18:36:17	GET	http://metasploitable.sait230.ca:80	/mutillidae/images/coykillericon.png		200 OK	Sp
62	2013/01/19 18:36:17	GET	http://metasploitable.sait230.ca:80	/mutillidae/images/backtrack-4-r2-logo-90-69.png		200 OK	Sp

Used 14.37 of 63.56MB

Spidering a Website - WGET

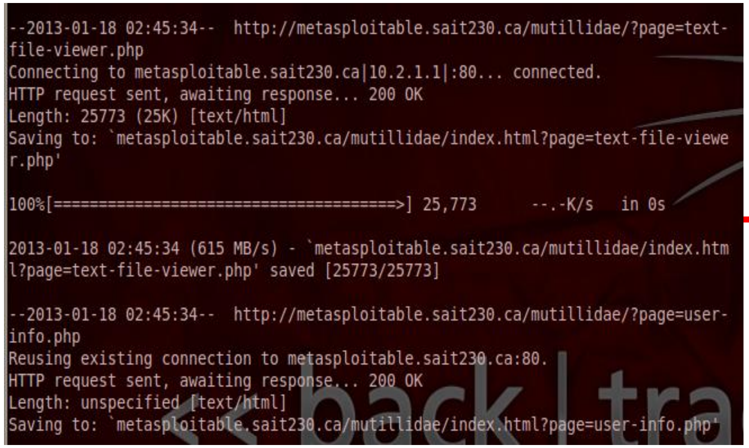
Mapping

- It is a console-based web browser;
- Runs on most platforms and has basic spidering capabilities;
- Wget will see each of the items retrieved.

Syntax

#wget [options] www.sait230.ca

```
root@bt# wget –r metasploitable.sait230.ca
```

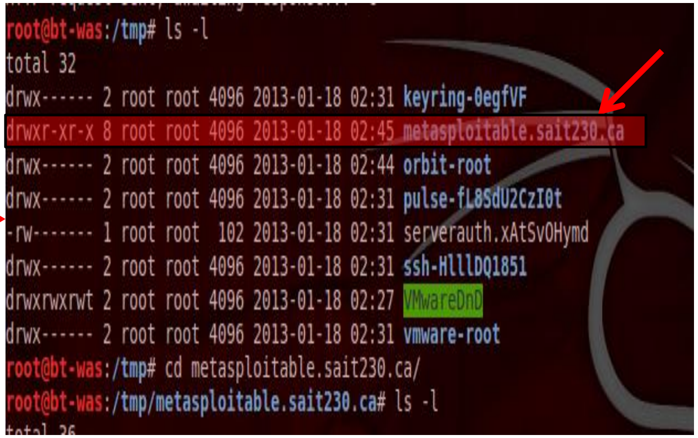


```
--2013-01-18 02:45:34--  http://metasploitable.sait230.ca/mutillidae/?page=text-
file-viewer.php
Connecting to metasploitable.sait230.ca|10.2.1.1|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 25773 (25K) [text/html]
Saving to: `metasploitable.sait230.ca/mutillidae/index.html?page=text-file-viewe
r.php'

100%[======================================>] 25,773      --.-K/s   in 0s

2013-01-18 02:45:34 (615 MB/s) - `metasploitable.sait230.ca/mutillidae/index.htm
l?page=text-file-viewer.php' saved [25773/25773]

--2013-01-18 02:45:34--  http://metasploitable.sait230.ca/mutillidae/?page=user-
info.php
Reusing existing connection to metasploitable.sait230.ca:80.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: `metasploitable.sait230.ca/mutillidae/index.html?page=user-info.php'
```

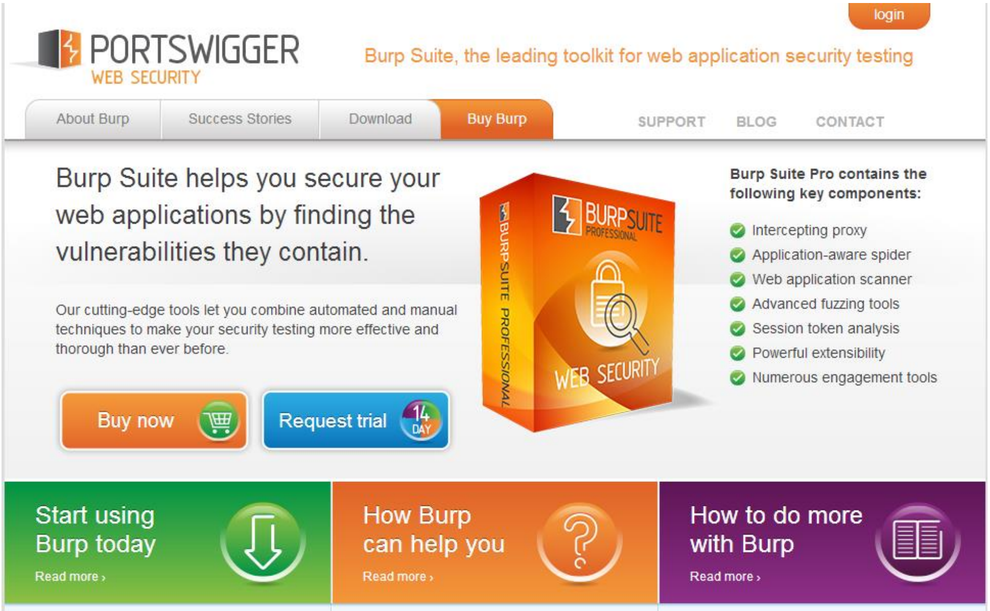


```
root@bt-was:/tmp# ls -l
total 32
drwx------ 2 root root 4096 2013-01-18 02:31 keyring-0egfVF
drwxr-xr-x 8 root root 4096 2013-01-18 02:45 metasploitable.sait230.ca
drwx------ 2 root root 4096 2013-01-18 02:44 orbit-root
drwx------ 2 root root 4096 2013-01-18 02:31 pulse-fL8SdU2CzI0t
-rw------- 1 root root  102 2013-01-18 02:31 serverauth.xAtSvOHymd
drwx------ 2 root root 4096 2013-01-18 02:31 ssh-HlllDQ1851
drwxrwxrwt 2 root root 4096 2013-01-18 02:27 VMwareDnD
drwx------ 2 root root 4096 2013-01-18 02:31 vmware-root
root@bt-was:/tmp# cd metasploitable.sait230.ca/
root@bt-was:/tmp/metasploitable.sait230.ca# ls -l
total 36
```

Burp Suite

Mapping

- Burp Suite is a collection of tools for web penetration testing;
- It includes spidering capability;
- Using the spider is similar to WebScarab;
- It's downloaded from portswigger.net;



Burp Suite, the leading toolkit for web application security testing

Burp Suite helps you secure your web applications by finding the vulnerabilities they contain.

Our cutting-edge tools let you combine automated and manual techniques to make your security testing more effective and thorough than ever before.

Burp Suite Pro contains the following key components:

- ✓ Intercepting proxy
- ✓ Application-aware spider
- ✓ Web application scanner
- ✓ Advanced fuzzing tools
- ✓ Session token analysis
- ✓ Powerful extensibility
- ✓ Numerous engagement tools

Start using Burp today
Read more ›

How Burp can help you
Read more ›

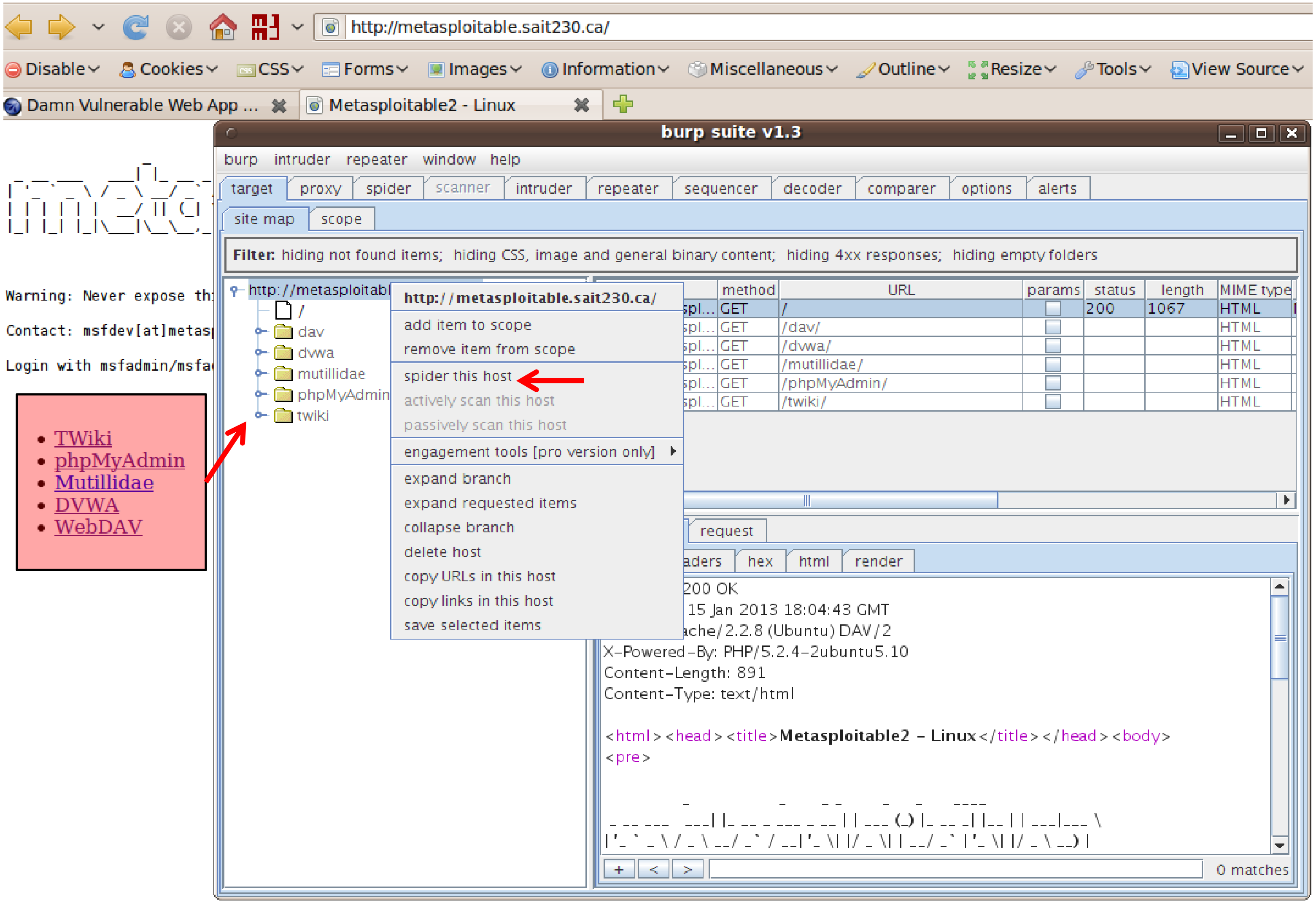
How to do more with Burp
Read more ›

Burp Suite

- Java application that can be used to secure or crack web applications;
- When Burp suite is used as a proxy server and a web browser uses this proxy server, it is possible to have control of all traffic that is exchanged between the web browser and web servers;
- Burp makes it possible to manipulate data before it is sent to the web server;
- Proxy Server, Spider, Intruder, Repeater.

Burp Suite

Mapping



http://metasploitable.sait230.ca/

Warning: Never expose th

Contact: msfdev[at]metas

Login with msfadmin/msfa

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

Filter: hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

	method	URL	params	status	length	MIME type
spl...	GET	/	□	200	1067	HTML
spl...	GET	/dav/	□			HTML
spl...	GET	/dvwa/	□			HTML
spl...	GET	/mutillidae/	□			HTML
spl...	GET	/phpMyAdmin/	□			HTML
spl...	GET	/twiki/	□			HTML

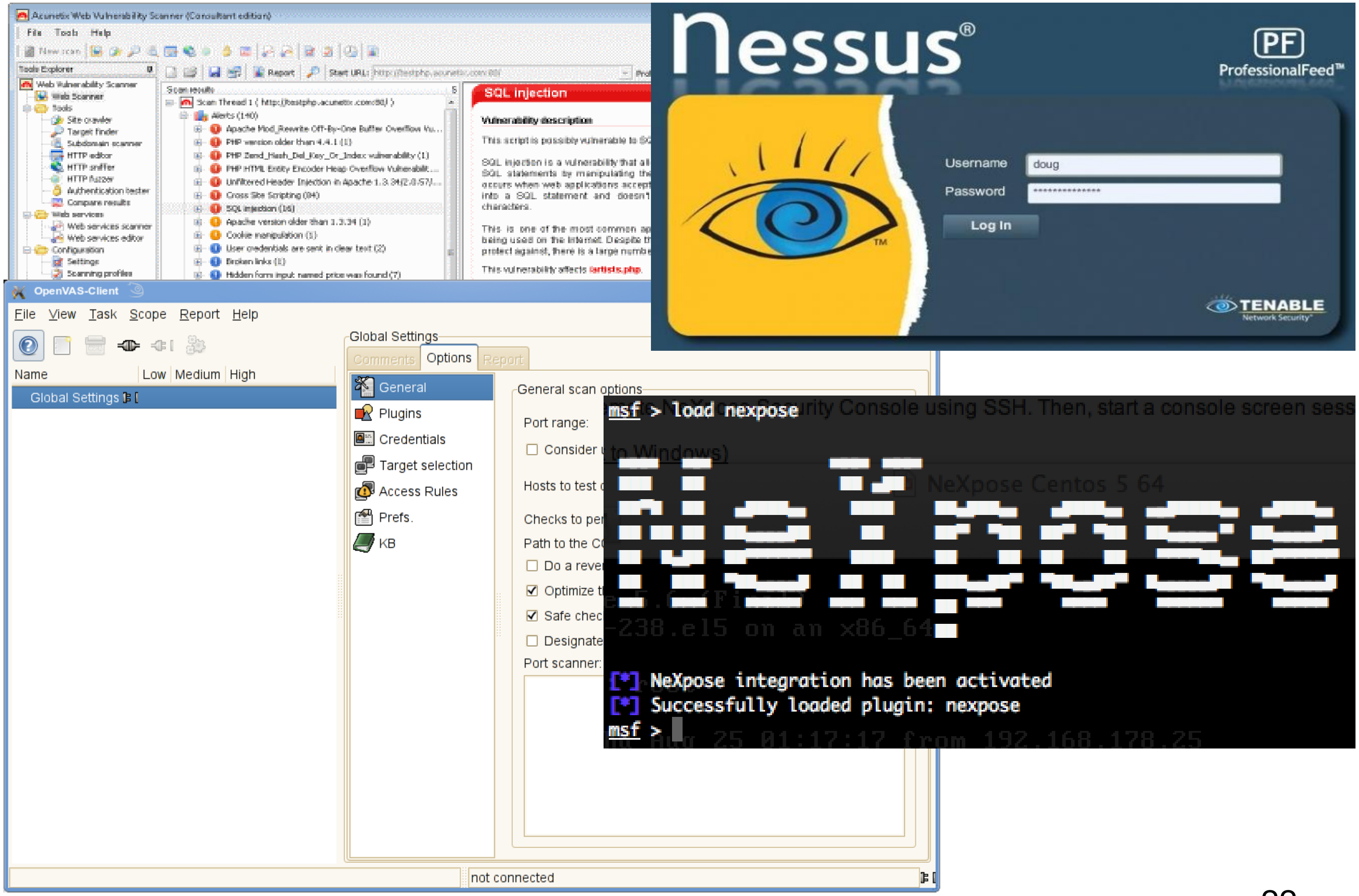
```
200 OK
 15 Jan 2013 18:04:43 GMT
ache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>
```

Vulnerability Identification

Discovering

Vulnerability Scanners



Acunetix Web Vulnerability Scanner (Consultant edition)

Scan Thread 1 (http://testphp.acunetix.com:80/)
Alerts (140)
- Apache Mod_Rewrite Off-By-One Buffer Overflow Vu...
- PHP version older than 4.4.1 (1)
- PHP Zend_Hash_Del_Key_Or_Index vulnerability (1)
- PHP HTML Entity Encoder Heap Overflow Vulnerabilit...
- Unfiltered Header Injection in Apache 1.3.34/2.0.57/...
- Cross Site Scripting (84)
- SQL injection (16)
- Apache version older than 1.3.34 (1)
- Cookie manipulation (1)
- User credentials are sent in clear text (2)
- Broken links (1)
- Hidden form input named price was found (7)

SQL injection

Vulnerability description

This script is possibly vulnerable to SQ

SQL injection is a vulnerability that al
SQL statements by manipulating the
occurs when web applications accept
into a SQL statement and doesn't
characters.

This is one of the most common ap
being used on the Internet. Despite th
protect against, there is a large numbe

This vulnerability affects /artists.php.

Nessus® ProfessionalFeed™

Username: doug
Password: ***************

OpenVAS-Client

General scan options

Port range:

☐ Consider

Hosts to test

Checks to per

Path to the C

☐ Do a rever

☑ Optimize t

☑ Safe chec

☐ Designate

Port scanner:

not connected

```
msf > load nexpose

[*] NeXpose integration has been activated
[*] Successfully loaded plugin: nexpose
msf >
```

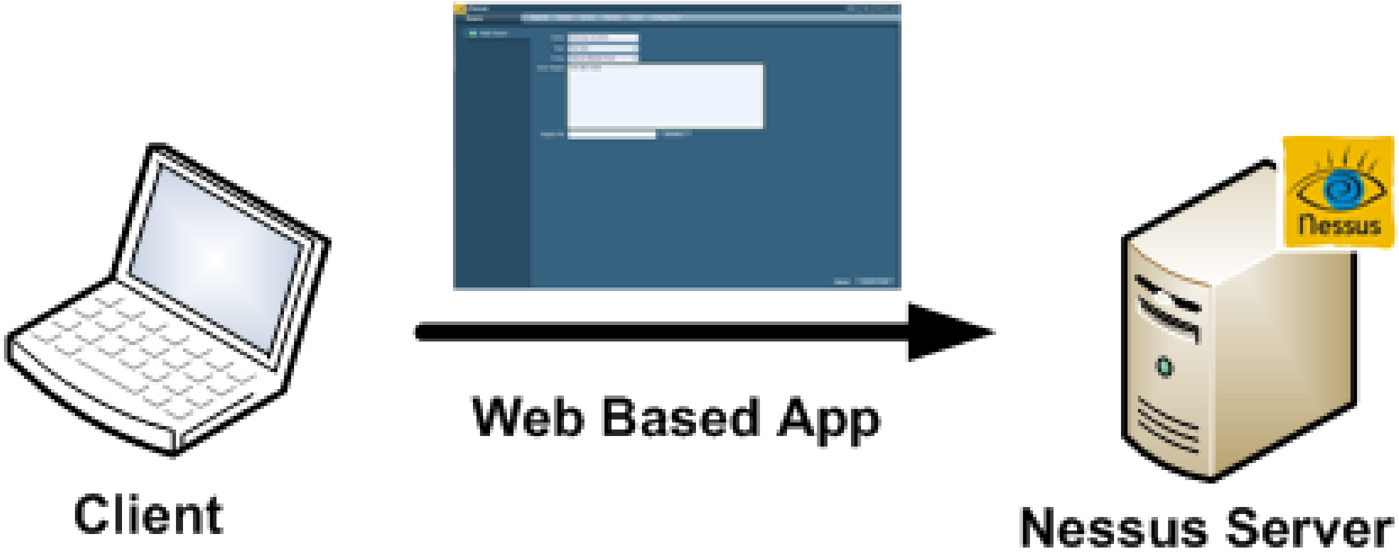
Vulnerability Scanning - Nessus

- One of the most popular scanning tools;
- It is free of charge for personal use in a non-enterprise environment (limited number of assets);
- Remote Data Gathering , Host Identification, Port Scanning are the main purposes of using this tool;
- Nessus will indicate the threat level for services or vulnerabilities it detects:
  - Low severity – Notification of issues
  - Medium severity – Warnings to think about
  - High severity – Issues that should be resolved
  - Critical severity – The issue has to be resolved
- Description of vulnerability;
- Risk factor;
- CVE (Common Vulnerability and Exposure) number.

Vulnerability Scanning - Nessus

Discovering

Nessus Architecture

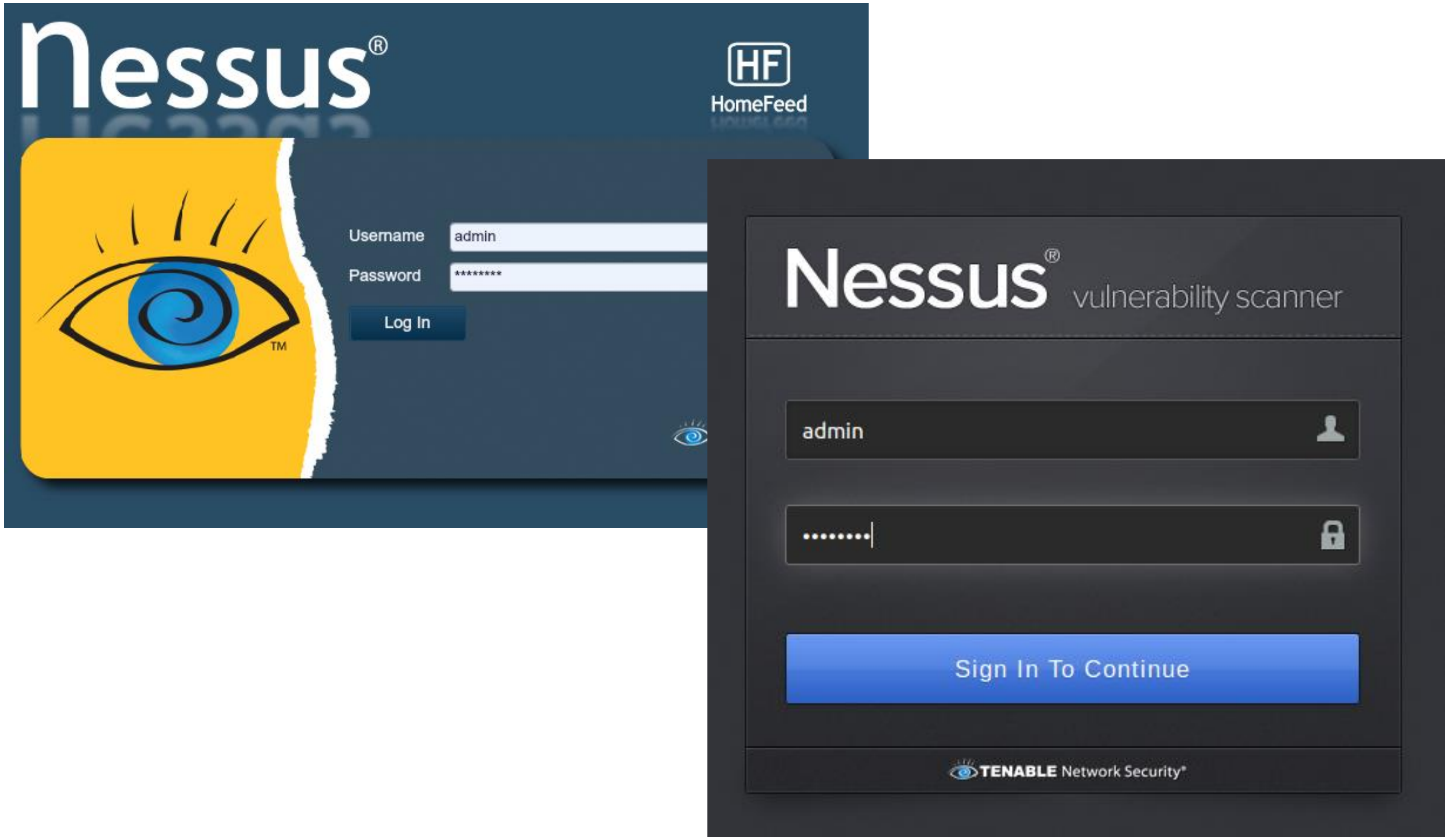


https://ip_address:8834

Vulnerability Scanning - Nessus

Discovering

https://192.168.X.XX:8834/



Username admin

Password ********

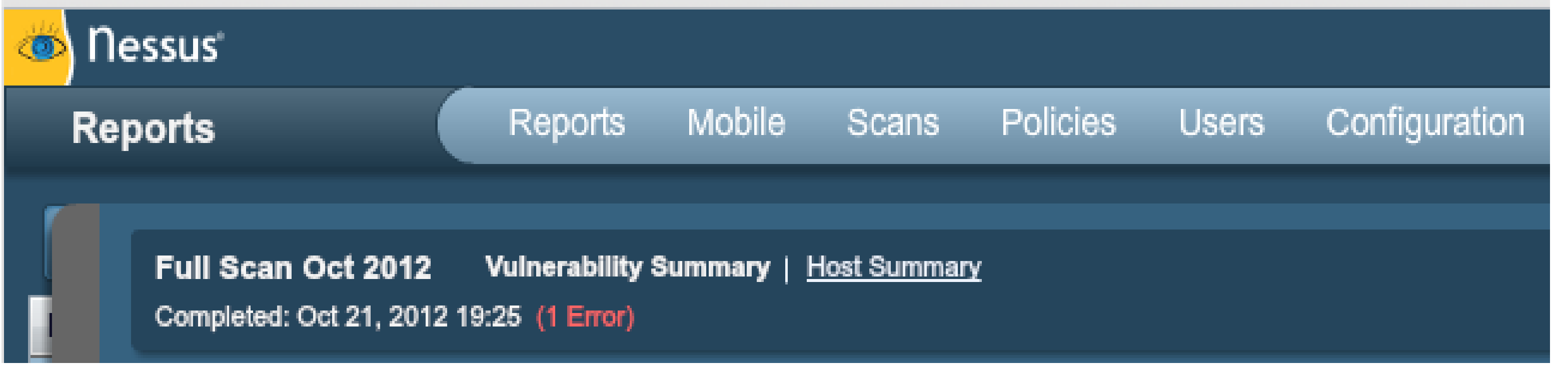
admin

•••••••••

Discovering

Vulnerability Scanning - Nessus

https://192.168.X.XX:8834/



Full Scan Oct 2012 Vulnerability Summary | Host Summary

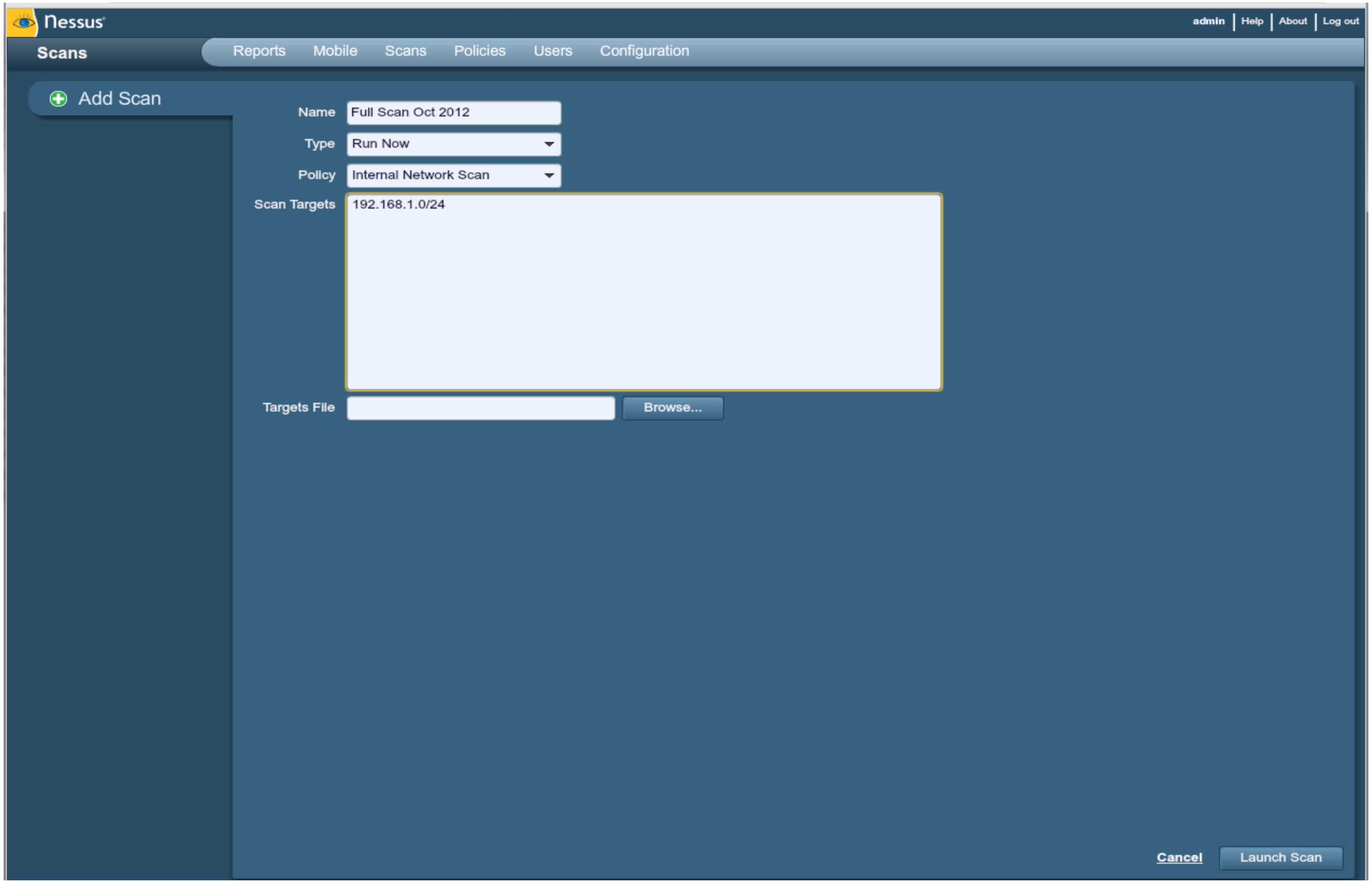
Completed: Oct 21, 2012 19:25 (1 Error)

- Results;
- Mobile;
- Scans;
- Policies;
- Users;
- Configuration.

Vulnerability Scanning - Nessus

Discovering

Scans



Nessus
admin | Help | About | Log out
Scans
Reports Mobile Scans Policies Users Configuration
Add Scan
Browse...
Cancel
Launch Scan

Name: Full Scan Oct 2012

Type: Run Now

Policy: Internal Network Scan

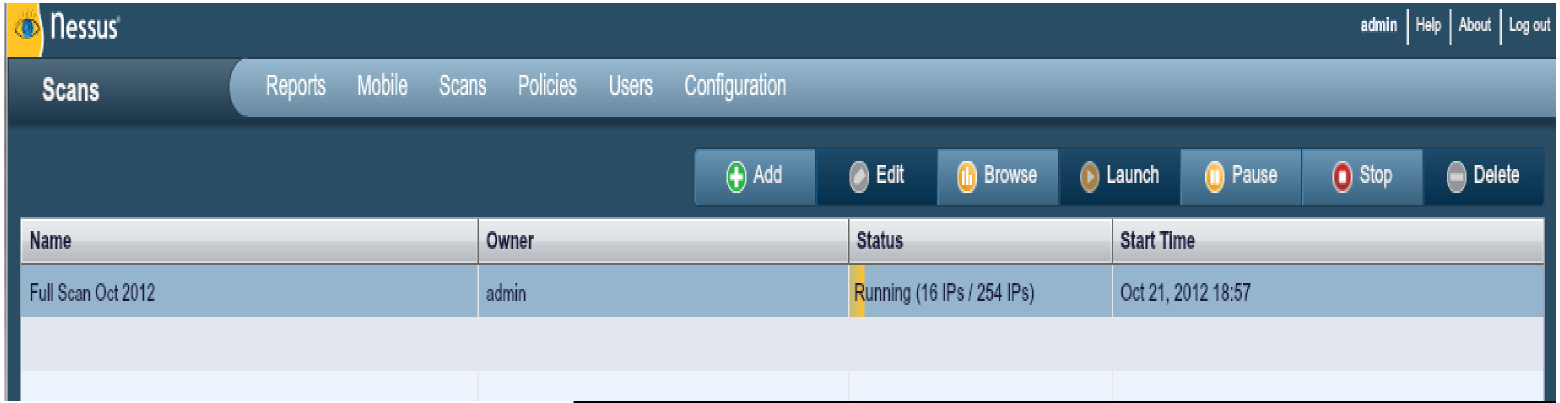
Scan Targets: 192.168.1.0/24

Targets File:

Vulnerability Scanning - Nessus

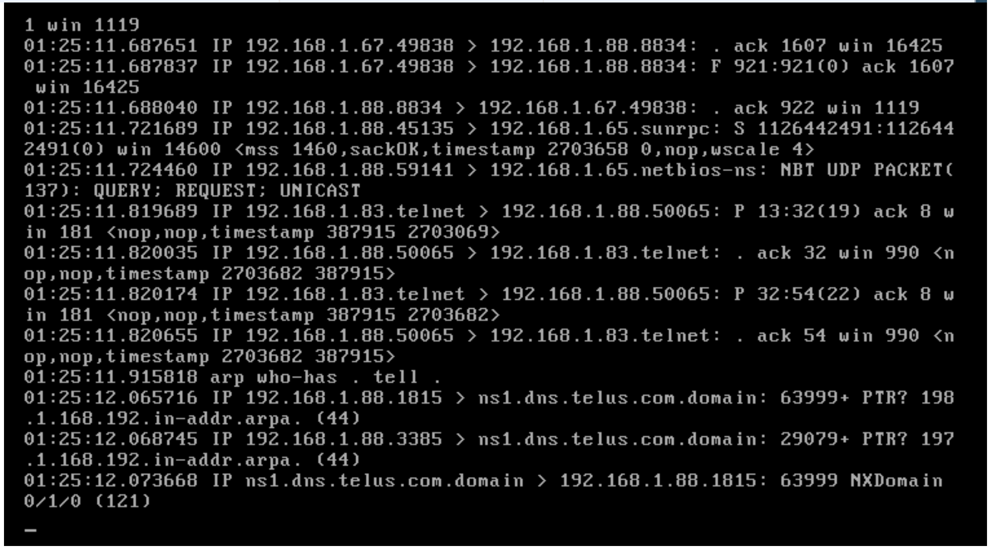
Discovering

Scanning



Name	Owner	Status	Start Time
Full Scan Oct 2012	admin	Running (16 IPs / 254 IPs)	Oct 21, 2012 18:57

tcpdump on the target computer



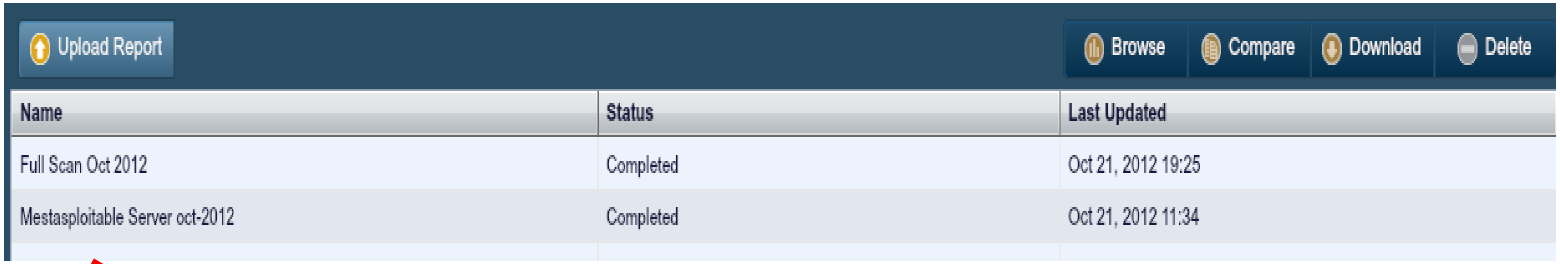
```
1 win 1119
01:25:11.687651 IP 192.168.1.67.49838 > 192.168.1.88.8834: . ack 1607 win 16425
01:25:11.687837 IP 192.168.1.67.49838 > 192.168.1.88.8834: F 921:921(0) ack 1607
 win 16425
01:25:11.688040 IP 192.168.1.88.8834 > 192.168.1.67.49838: . ack 922 win 1119
01:25:11.721689 IP 192.168.1.88.45135 > 192.168.1.65.sunrpc: S 1126442491:112644
2491(0) win 14600 <mss 1460,sackOK,timestamp 2703658 0,nop,wscale 4>
01:25:11.724460 IP 192.168.1.88.59141 > 192.168.1.65.netbios-ns: NBT UDP PACKET(
137): QUERY; REQUEST; UNICAST
01:25:11.819689 IP 192.168.1.83.telnet > 192.168.1.88.50065: P 13:32(19) ack 8 w
in 181 <nop,nop,timestamp 387915 2703069>
01:25:11.820035 IP 192.168.1.88.50065 > 192.168.1.83.telnet: . ack 32 win 990 <n
op,nop,timestamp 2703682 387915>
01:25:11.820174 IP 192.168.1.83.telnet > 192.168.1.88.50065: P 32:54(22) ack 8 w
in 181 <nop,nop,timestamp 387915 2703682>
01:25:11.820655 IP 192.168.1.88.50065 > 192.168.1.83.telnet: . ack 54 win 990 <n
op,nop,timestamp 2703682 387915>
01:25:11.915818 arp who-has . tell .
01:25:12.065716 IP 192.168.1.88.1815 > ns1.dns.telus.com.domain: 63999+ PTR? 198
.1.168.192.in-addr.arpa. (44)
01:25:12.068745 IP 192.168.1.88.3385 > ns1.dns.telus.com.domain: 29079+ PTR? 197
.1.168.192.in-addr.arpa. (44)
01:25:12.073668 IP ns1.dns.telus.com.domain > 192.168.1.88.1815: 63999 NXDomain
0/1/0 (121)

_
```

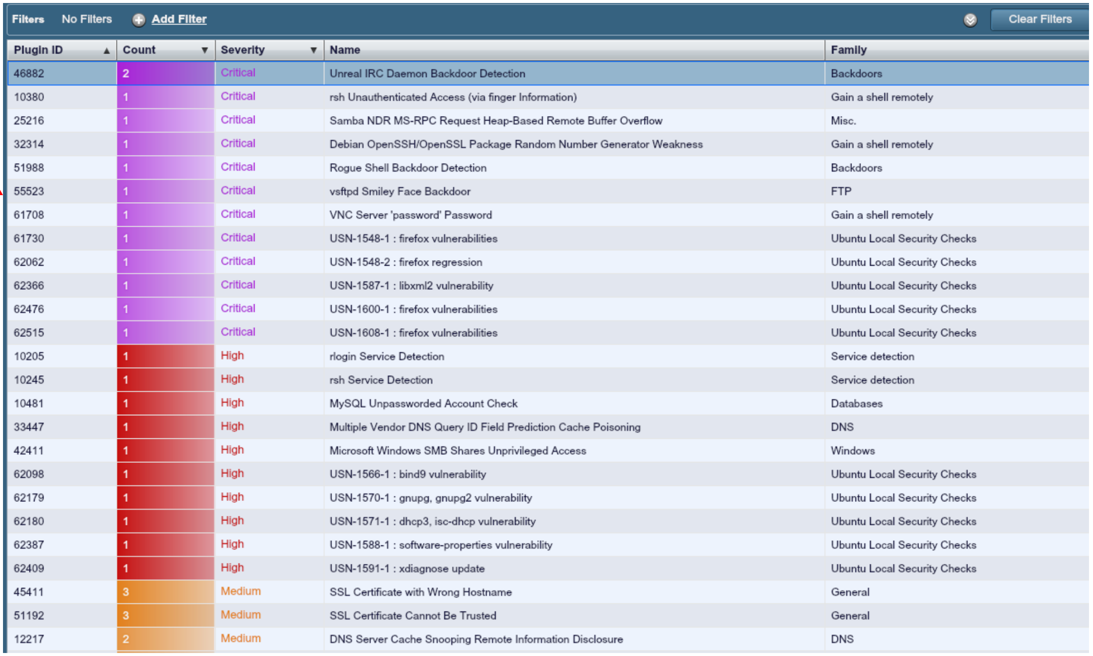
Vulnerability Scanning - Nessus

Discovering

Results



Name	Status	Last Updated
Full Scan Oct 2012	Completed	Oct 21, 2012 19:25
Mestasploitable Server oct-2012	Completed	Oct 21, 2012 11:34

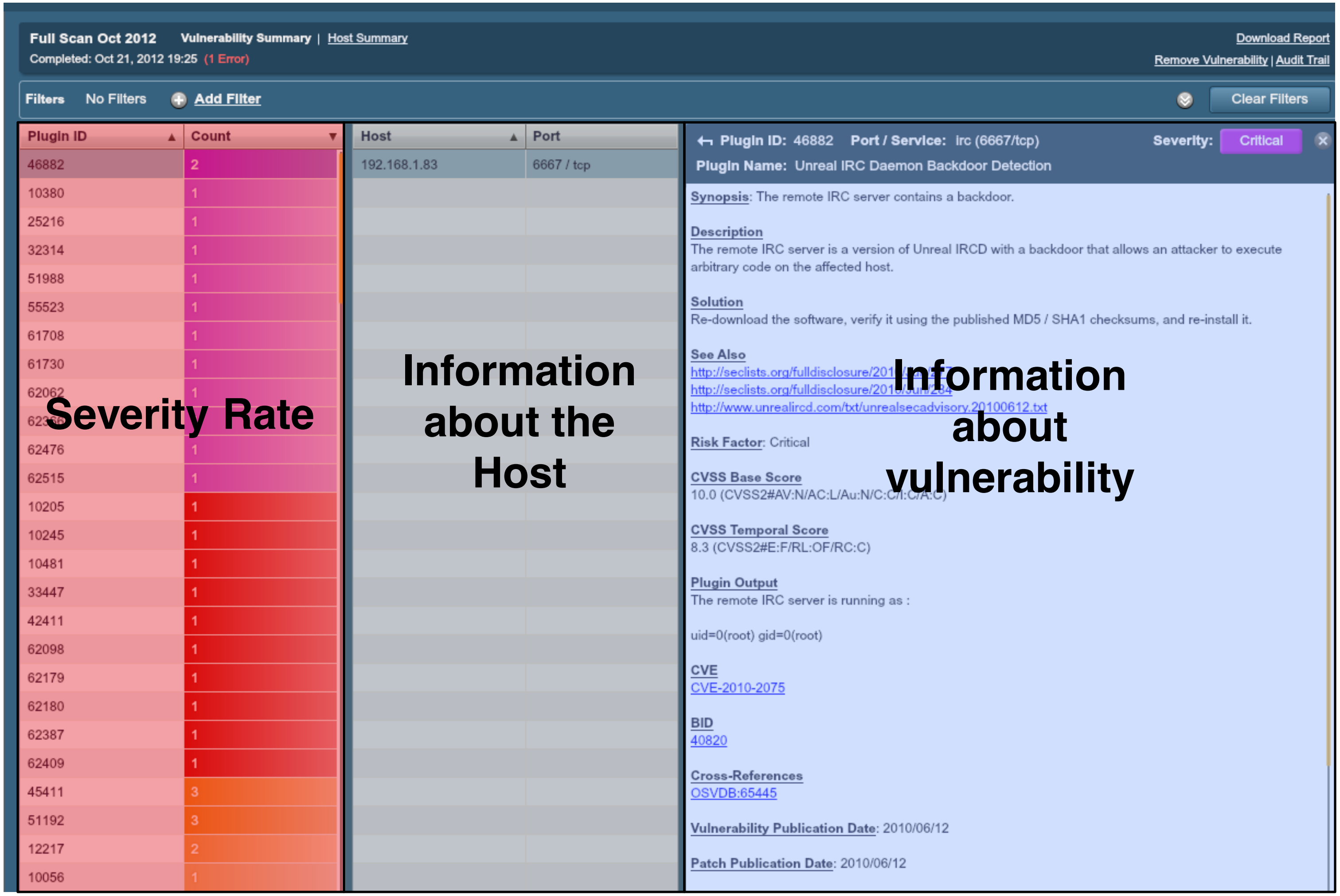


Plugin ID ▲	Count ▼	Severity ▼	Name	Family
46882	2	Critical	Unreal IRC Daemon Backdoor Detection	Backdoors
10380	1	Critical	rsh Unauthenticated Access (via finger Information)	Gain a shell remotely
25216	1	Critical	Samba NDR MS-RPC Request Heap-Based Remote Buffer Overflow	Misc.
32314	1	Critical	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	Gain a shell remotely
51988	1	Critical	Rogue Shell Backdoor Detection	Backdoors
55523	1	Critical	vsftpd Smiley Face Backdoor	FTP
61708	1	Critical	VNC Server 'password' Password	Gain a shell remotely
61730	1	Critical	USN-1548-1 : firefox vulnerabilities	Ubuntu Local Security Checks
62062	1	Critical	USN-1548-2 : firefox regression	Ubuntu Local Security Checks
62366	1	Critical	USN-1587-1 : libxml2 vulnerability	Ubuntu Local Security Checks
62476	1	Critical	USN-1600-1 : firefox vulnerabilities	Ubuntu Local Security Checks
62515	1	Critical	USN-1608-1 : firefox vulnerabilities	Ubuntu Local Security Checks
10205	1	High	rlogin Service Detection	Service detection
10245	1	High	rsh Service Detection	Service detection
10481	1	High	MySQL Unpassworded Account Check	Databases
33447	1	High	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning	DNS
42411	1	High	Microsoft Windows SMB Shares Unprivileged Access	Windows
62098	1	High	USN-1566-1 : bind9 vulnerability	Ubuntu Local Security Checks
62179	1	High	USN-1570-1 : gnupg, gnupg2 vulnerability	Ubuntu Local Security Checks
62180	1	High	USN-1571-1 : dhcp3, isc-dhcp vulnerability	Ubuntu Local Security Checks
62387	1	High	USN-1588-1 : software-properties vulnerability	Ubuntu Local Security Checks
62409	1	High	USN-1591-1 : xdiagnose update	Ubuntu Local Security Checks
45411	3	Medium	SSL Certificate with Wrong Hostname	General
51192	3	Medium	SSL Certificate Cannot Be Trusted	General
12217	2	Medium	DNS Server Cache Snooping Remote Information Disclosure	DNS

Vulnerability Scanning - Nessus

Discovering

Results



Full Scan Oct 2012 **Vulnerability Summary** | Host Summary

Completed: Oct 21, 2012 19:25 (1 Error)

Download Report

Remove Vulnerability | Audit Trail

Filters No Filters ⊕ Add Filter

Clear Filters

Plugin ID ▲	Count ▼
46882	2
10380	1
25216	1
32314	1
51988	1
55523	1
61708	1
61730	1
62062	1
62366	1
62476	1
62515	1
10205	1
10245	1
10481	1
33447	1
42411	1
62098	1
62179	1
62180	1
62387	1
62409	1
45411	3
51192	3
12217	2
10056	1

Host ▲	Port
192.168.1.83	6667 / tcp

Plugin ID: 46882 **Port / Service:** irc (6667/tcp) **Severity:** Critical

Plugin Name: Unreal IRC Daemon Backdoor Detection

Synopsis: The remote IRC server contains a backdoor.

Description
The remote IRC server is a version of Unreal IRCD with a backdoor that allows an attacker to execute arbitrary code on the affected host.

Solution
Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

See Also
http://seclists.org/fulldisclosure/2010/Jun/277
http://seclists.org/fulldisclosure/2010/Jun/284
http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt

Risk Factor: Critical

CVSS Base Score
10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score
8.3 (CVSS2#E:F/RL:OF/RC:C)

Plugin Output
The remote IRC server is running as :

uid=0(root) gid=0(root)

CVE
CVE-2010-2075

BID
40820

Cross-References
OSVDB:65445

Vulnerability Publication Date: 2010/06/12

Patch Publication Date: 2010/06/12

Severity Rate

Information about the Host

Information about vulnerability

Vulnerability Scanning - Nessus

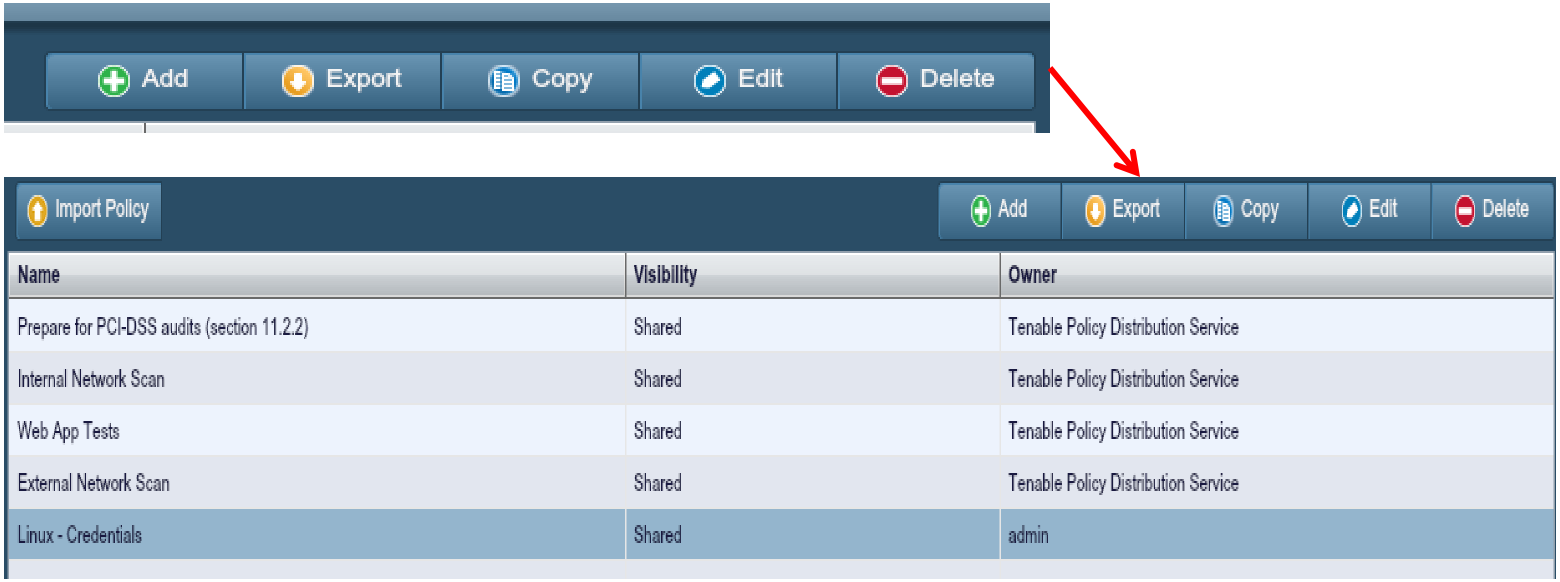
Discovering

critical	Intruders **can easily gain** control of the host, which can lead to the compromise of your entire network security. For example, full read and write access to files, remote execution of commands, and the presence of backdoors.
high	Intruders **can possibly gain** control of the host, or there may be potential leakage of highly sensitive information. For example, full read access to files, potential backdoors, or a listing of all the users on the host.
medium	Intruders **may be able to gain** access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, partial disclosure of file contents, access to certain files on the host, directory browsing.
Low	Intruders **may be able to collect** sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
Info	Intruders **can collect information** about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.

Vulnerability Scanning - Nessus

Discovering

Policies

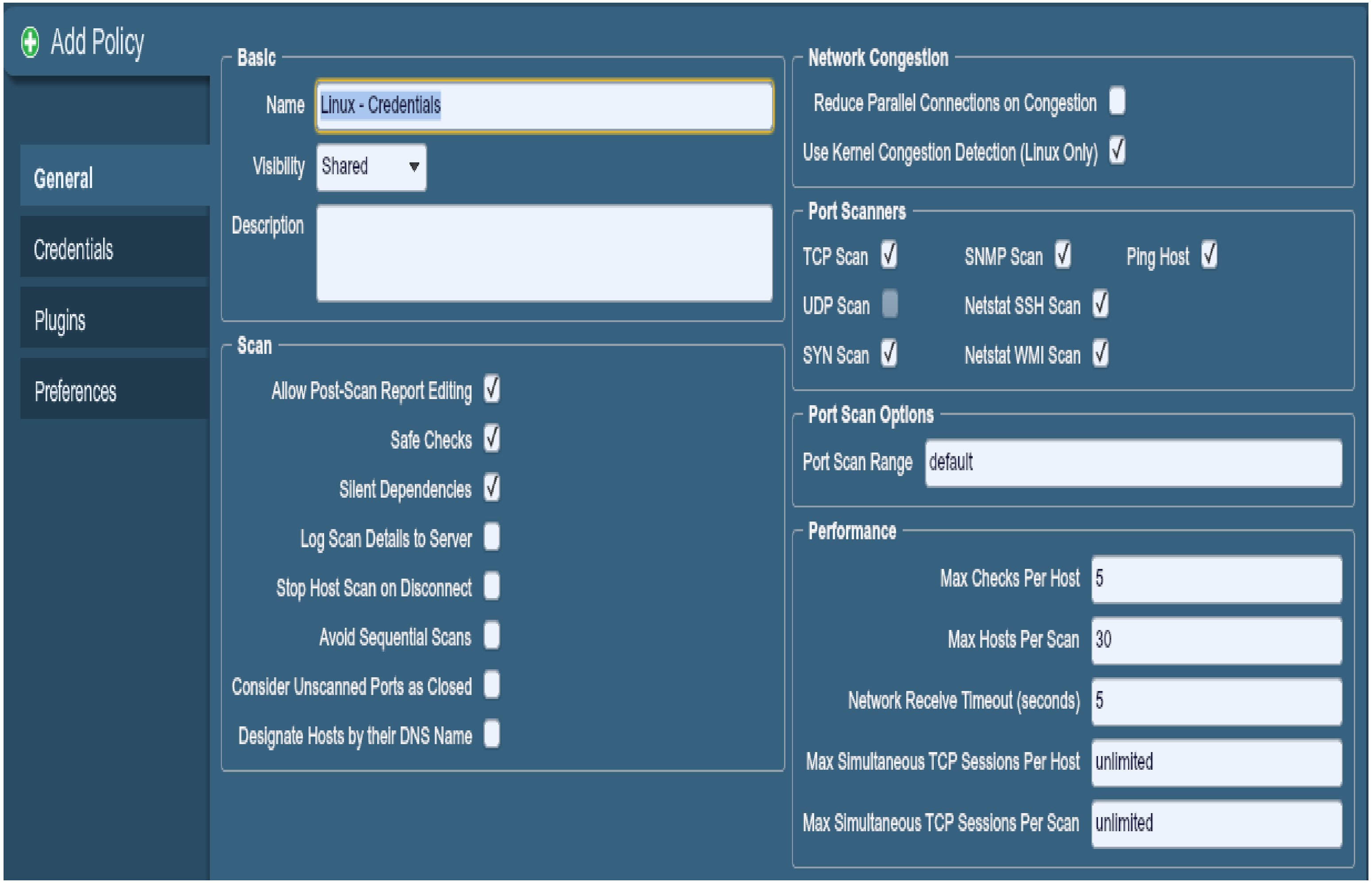


Name	Visibility	Owner
Prepare for PCI-DSS audits (section 11.2.2)	Shared	Tenable Policy Distribution Service
Internal Network Scan	Shared	Tenable Policy Distribution Service
Web App Tests	Shared	Tenable Policy Distribution Service
External Network Scan	Shared	Tenable Policy Distribution Service
Linux - Credentials	Shared	admin

Vulnerability Scanning - Nessus

Discovering

Policies



Basic

Name: Linux - Credentials

Visibility: Shared

Description:

Scan

Allow Post-Scan Report Editing ☑

Safe Checks ☑

Silent Dependencies ☑

Log Scan Details to Server ☐

Stop Host Scan on Disconnect ☐

Avoid Sequential Scans ☐

Consider Unscanned Ports as Closed ☐

Designate Hosts by their DNS Name ☐

Network Congestion

Reduce Parallel Connections on Congestion ☐

Use Kernel Congestion Detection (Linux Only) ☑

Port Scanners

TCP Scan ☑ SNMP Scan ☑ Ping Host ☑

UDP Scan ☐ Netstat SSH Scan ☑

SYN Scan ☑ Netstat WMI Scan ☑

Port Scan Options

Port Scan Range: default

Performance

Max Checks Per Host: 5

Max Hosts Per Scan: 30

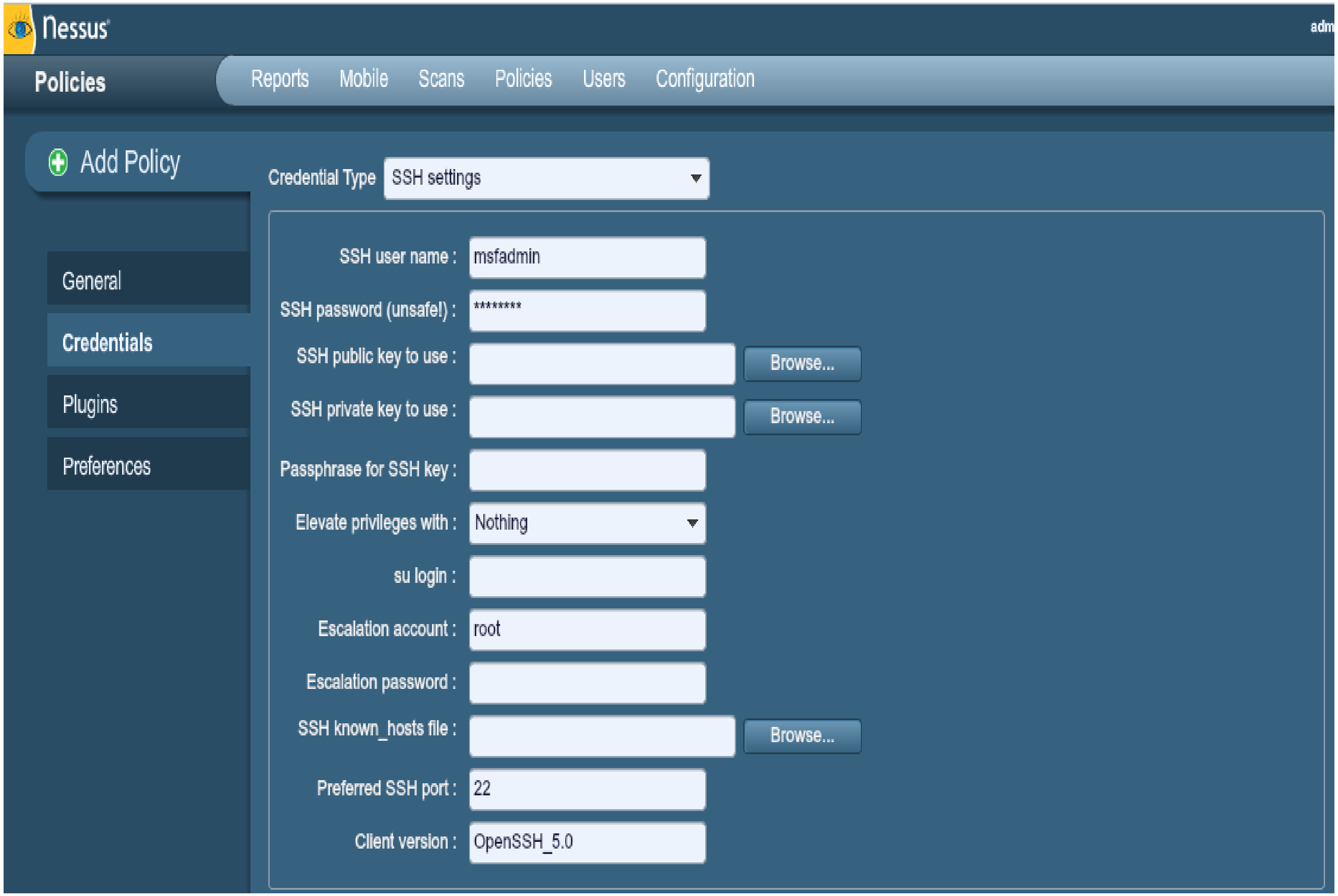
Network Receive Timeout (seconds): 5

Max Simultaneous TCP Sessions Per Host: unlimited

Max Simultaneous TCP Sessions Per Scan: unlimited

Vulnerability Scanning - Nessus

Policies



Credential Type: SSH settings

SSH user name : msfadmin

SSH password (unsafe!) : ********

SSH public key to use :

SSH private key to use :

Passphrase for SSH key :

Elevate privileges with : Nothing

su login :

Escalation account : root

Escalation password :

SSH known_hosts file :

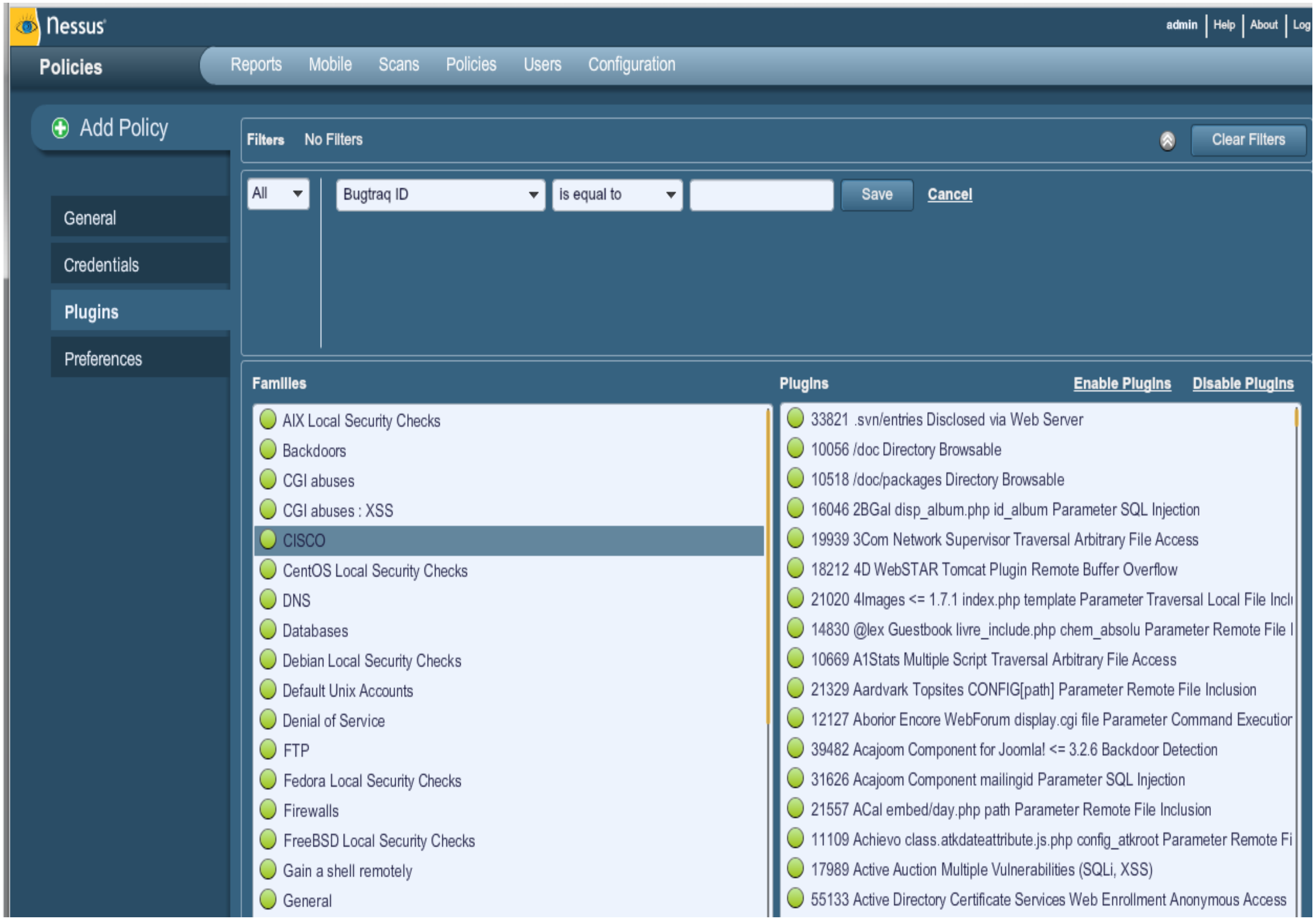
Preferred SSH port : 22

Client version : OpenSSH_5.0

Vulnerability Scanning - Nessus

Discovering

Policies



Filters No Filters

All | Bugtraq ID | is equal to

Families

- AIX Local Security Checks
- Backdoors
- CGI abuses
- CGI abuses : XSS
- CISCO
- CentOS Local Security Checks
- DNS
- Databases
- Debian Local Security Checks
- Default Unix Accounts
- Denial of Service
- FTP
- Fedora Local Security Checks
- Firewalls
- FreeBSD Local Security Checks
- Gain a shell remotely
- General

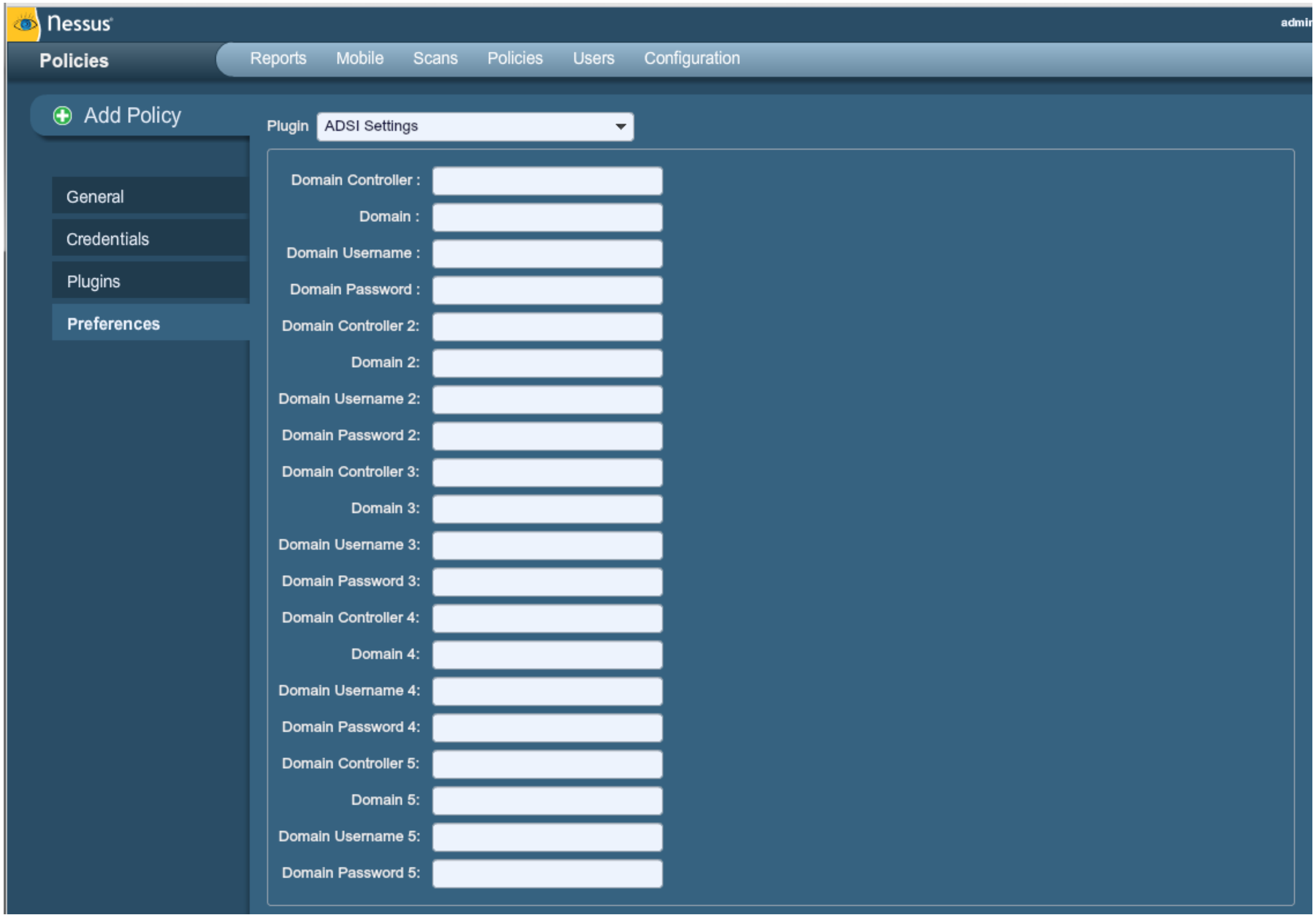
Plugins

- 33821 .svn/entries Disclosed via Web Server
- 10056 /doc Directory Browsable
- 10518 /doc/packages Directory Browsable
- 16046 2BGal disp_album.php id_album Parameter SQL Injection
- 19939 3Com Network Supervisor Traversal Arbitrary File Access
- 18212 4D WebSTAR Tomcat Plugin Remote Buffer Overflow
- 21020 4Images <= 1.7.1 index.php template Parameter Traversal Local File Incl
- 14830 @lex Guestbook livre_include.php chem_absolu Parameter Remote File I
- 10669 A1Stats Multiple Script Traversal Arbitrary File Access
- 21329 Aardvark Topsites CONFIG[path] Parameter Remote File Inclusion
- 12127 Aborior Encore WebForum display.cgi file Parameter Command Executior
- 39482 Acajoom Component for Joomla! <= 3.2.6 Backdoor Detection
- 31626 Acajoom Component mailingid Parameter SQL Injection
- 21557 ACal embed/day.php path Parameter Remote File Inclusion
- 11109 Achievo class.atkdateattribute.js.php config_atkroot Parameter Remote Fi
- 17989 Active Auction Multiple Vulnerabilities (SQLi, XSS)
- 55133 Active Directory Certificate Services Web Enrollment Anonymous Access

Vulnerability Scanning - Nessus

Discovering

Policies



Plugin: ADSI Settings

Domain Controller :

Domain :

Domain Username :

Domain Password :

Domain Controller 2:

Domain 2:

Domain Username 2:

Domain Password 2:

Domain Controller 3:

Domain 3:

Domain Username 3:

Domain Password 3:

Domain Controller 4:

Domain 4:

Domain Username 4:

Domain Password 4:

Domain Controller 5:

Domain 5:

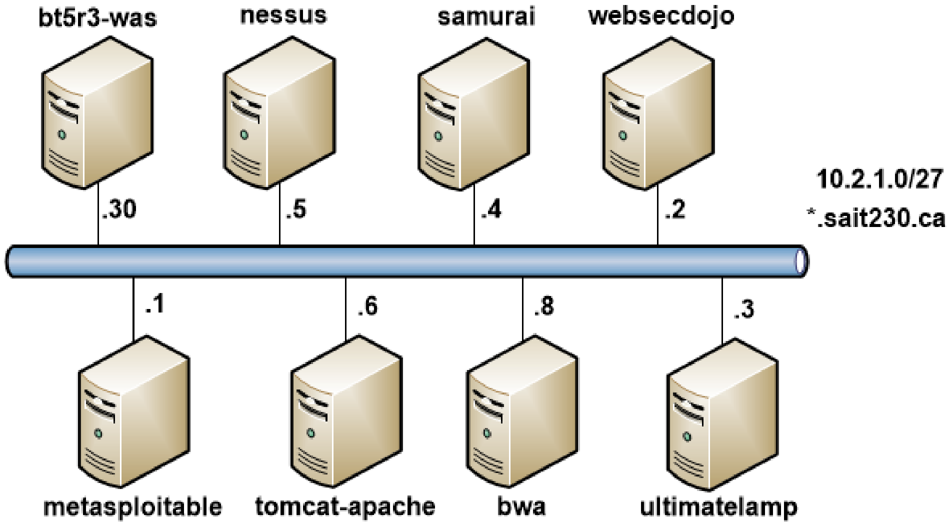
Domain Username 5:

Domain Password 5:

Project – Phase 1: Recon & Mapping

Mapping

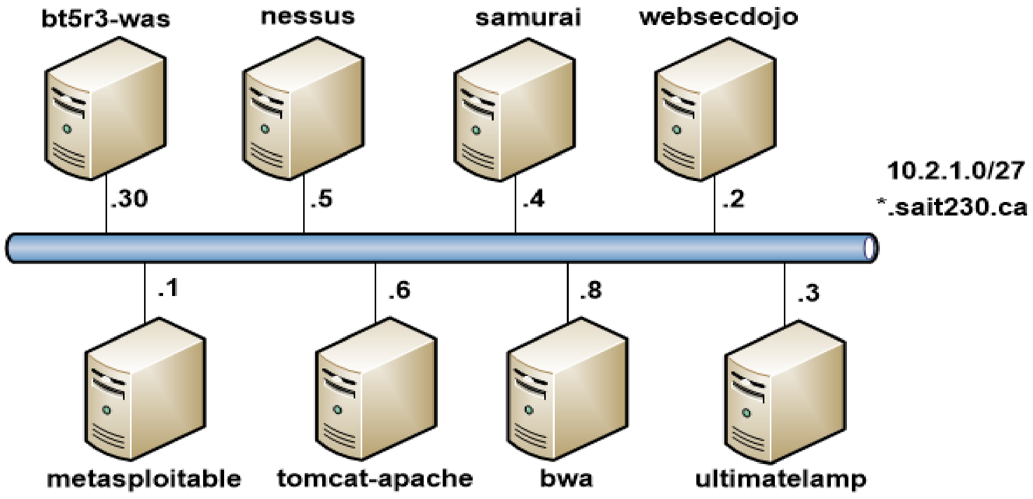
- Using WebScarab and Wget, please spider the following web sites:
  - metasploitable.sait230.ca;
  - bwa.sait230.ca;
  - websecdojo.sait230.ca.



Project – Phase 2: Discovery

Discovering

- Using Nessus, select the security template with Authentication enabled to scan all the network;
- Focus on the vulnerabilities on services associated with the ports requested on the previous Lab;
- Focus on ports: TCP 80, 808X, 800X, 8180, 443. (Tomcat, Apache and etc.)



Project – Phase 2: Discovery

Discovering

Hostname	IP	Vulnerabilities	Exploitable?

SAIT POLYTECHNIC

FURTHER
YOUR
PASSION

Questions