sait.ca

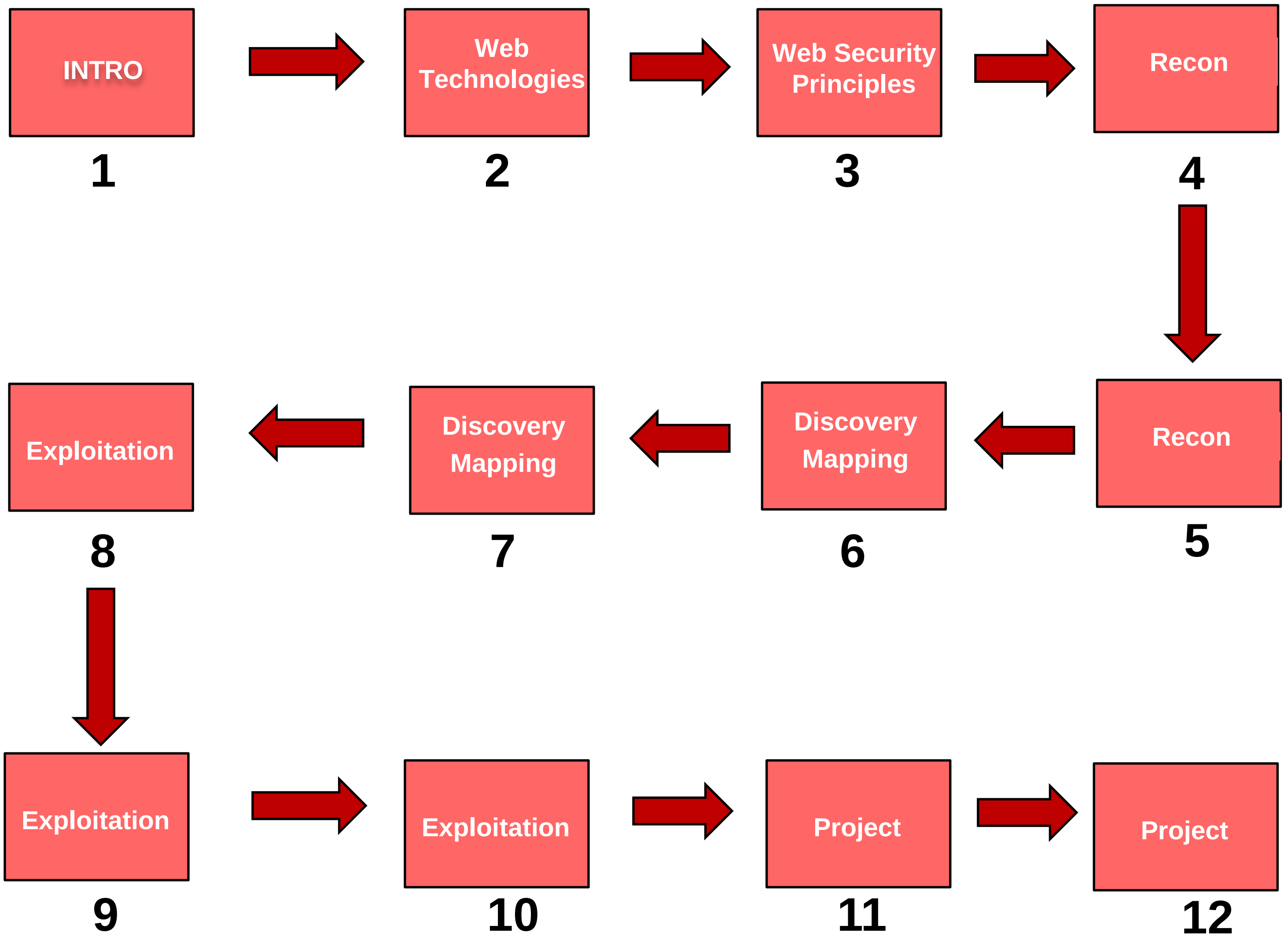
SAIT POLYTECHNIC

FURTHER YOUR PASSION

Web App & Data Base Security

Introduction

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

- About Web App & Data Base Security;
- The Project;
- About the Virtual Machines / Labs;
- LAB: Testing the Labs.

About Web App & Data Base Security

- **Day 1 (Introduction):** Show the plan and test the VMs;
- **Day 2 (Web App Technologies):** An introduction of the HTTP (s) protocols, Proxy / Web Content Filters, Vulnerability Assessment on the VMs,;
- **Day 3 (Web Security Principles):** Top 10 Security Attacks by OWASP, Starting the project;
- **Day 4 (Reconnaissance):** The first phase of the penetration testing methodology. Showing some interesting tools to gather some information about the target

About Web App & Data Base Security

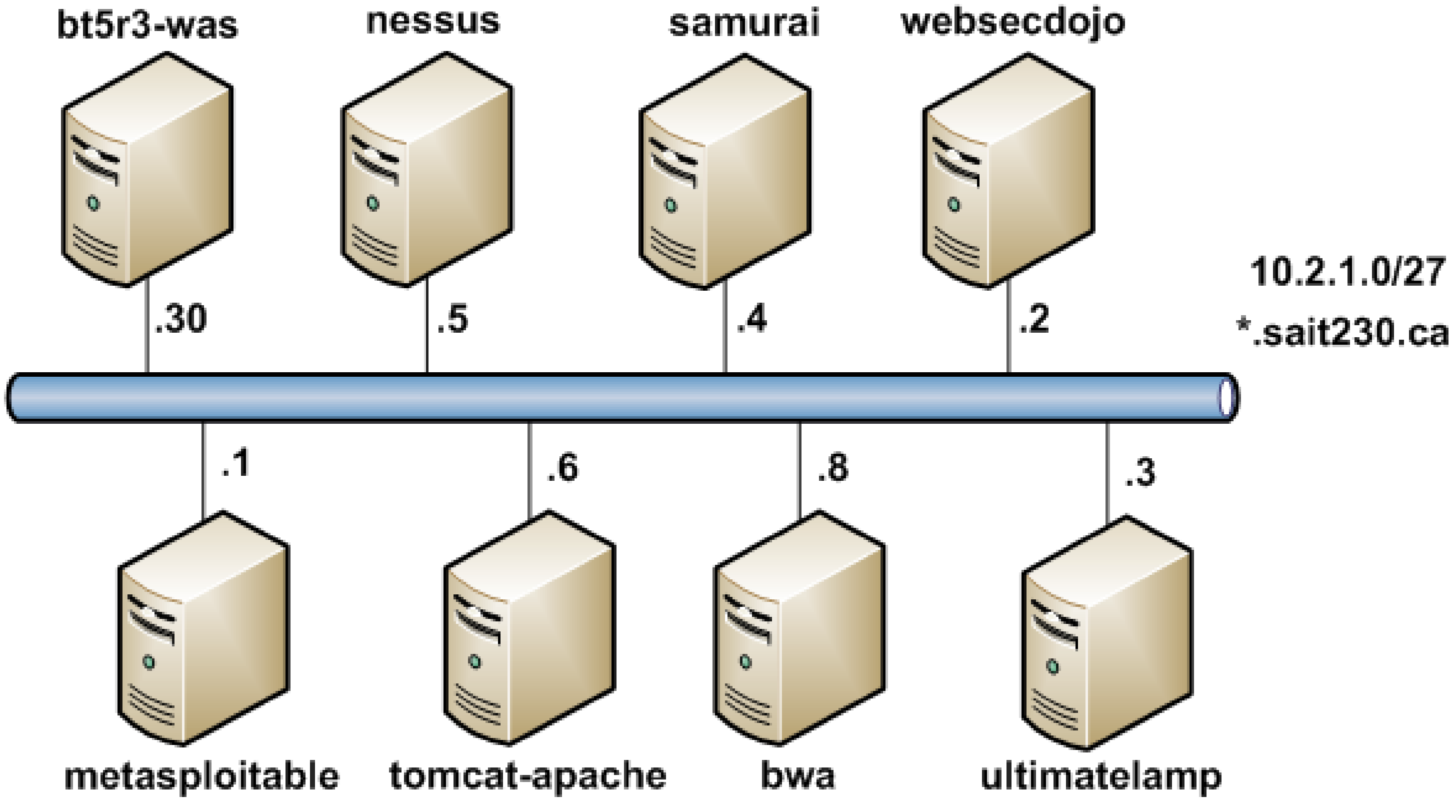
- **Day 5-6 (Discovery and Mapping):** The second phase of the penetration testing methodology. Using some tools to provide more information about the target's infrastructure;
- **Day 7-8 (Exploitation):** The final phase of penetration testing methodology. Testing exploitation techniques for SQL Injection, File Injection and Cross-Site Scripting (XSS)

The Project

Description: Create a report for the annual vulnerability and penetration testing exercise;

- The project will replace the exam;
- Maximum of 20 pages containing details for what you found on the network environment:
  1. Reconnaissance;
  2. Discovery;
  3. Mapping;
  4. Exploitation;
  5. Report (Executive and Technical).

Web App & Data Base Security - Lab



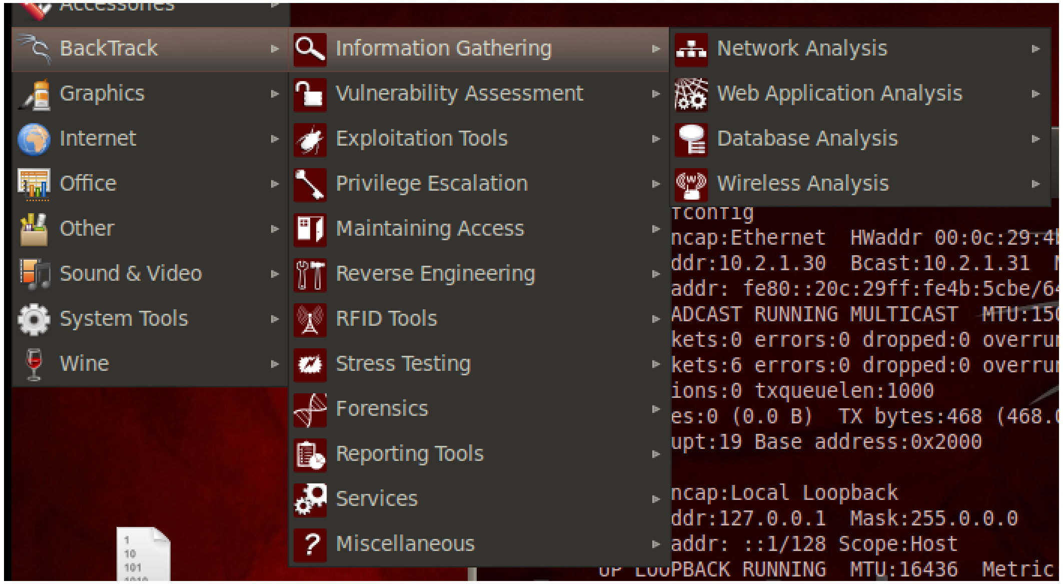
Web App & Data Base Security - Lab

- VMs preconfigured – copy and use them;
- Network configuration will remain the same – ***I moved it***;
- They will be available for download – test them at home.

About the Virtual Machines (VMs)

Backtrack 5r3 – bt5r3-was.sait230.ca

- Linux distribution with lots of security tools for security tests;
- Recon, Mapping, Discovery and Exploitation tools for Web App and Data Base Security;

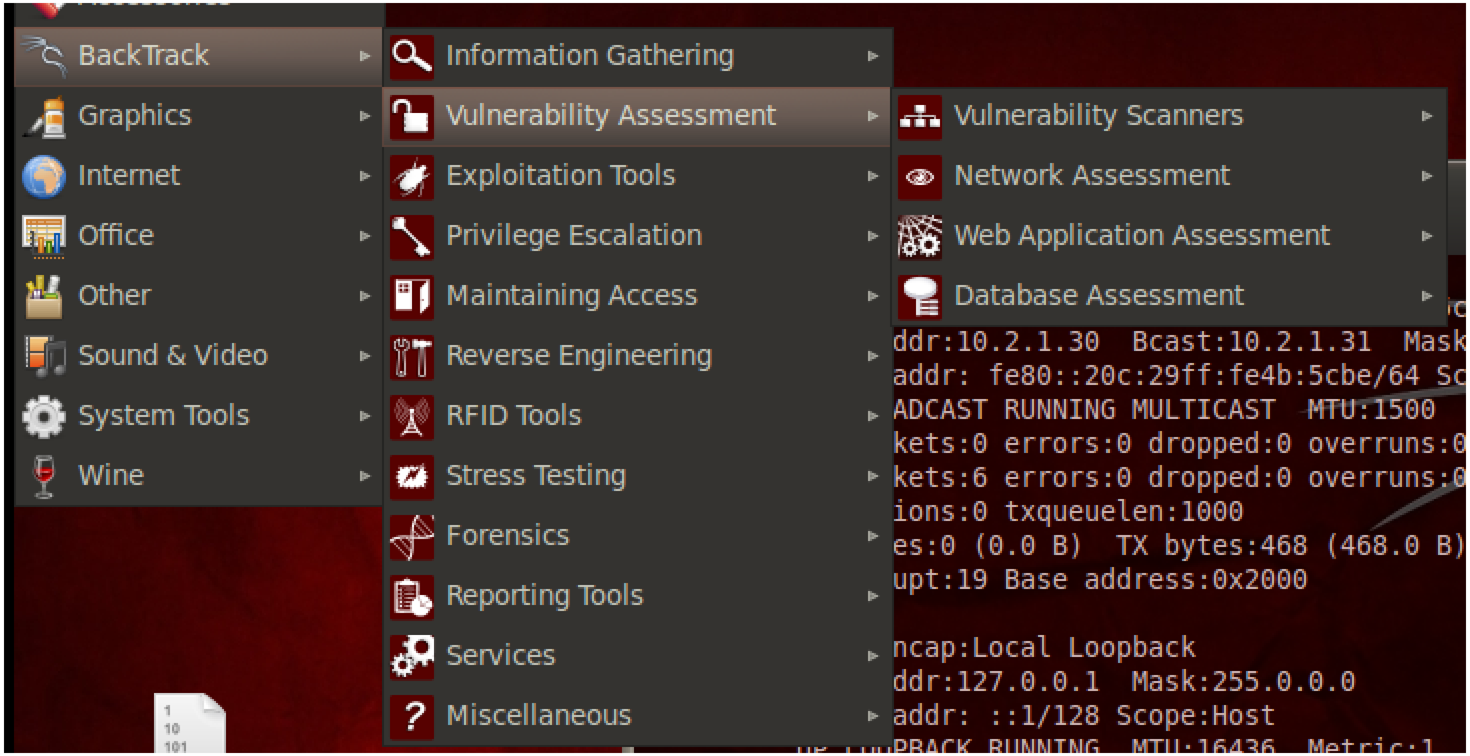


```
fconfig
ncap:Ethernet  HWaddr 00:0c:29:4b
ddr:10.2.1.30  Bcast:10.2.1.31  M
addr: fe80::20c:29ff:fe4b:5cbe/64
ADCAST RUNNING MULTICAST  MTU:150
kets:0 errors:0 dropped:0 overrun
kets:6 errors:0 dropped:0 overrun
ions:0 txqueuelen:1000
es:0 (0.0 B)  TX bytes:468 (468.0
upt:19 Base address:0x2000

ncap:Local Loopback
ddr:127.0.0.1  Mask:255.0.0.0
addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING  MTU:16436  Metric
```

About the Virtual Machines (VMs)

Backtrack 5r3 – bt5r3-was.sait230.ca



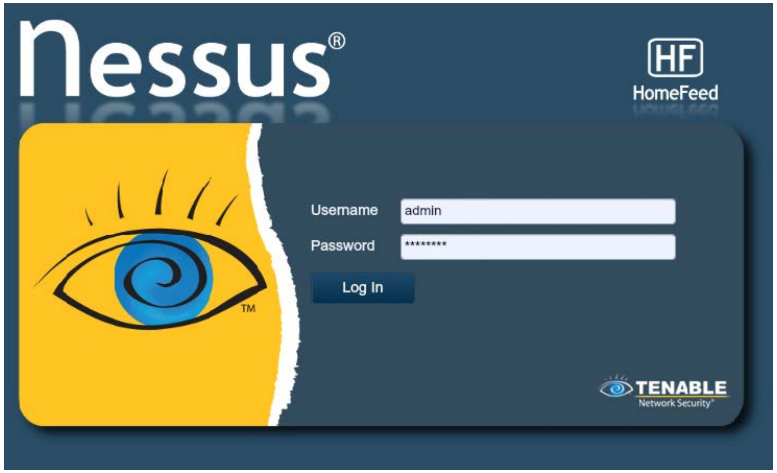
```
ddr:10.2.1.30  Bcast:10.2.1.31  Mask
addr: fe80::20c:29ff:fe4b:5cbe/64 Sc
ADCAST RUNNING MULTICAST  MTU:1500
kets:0 errors:0 dropped:0 overruns:0
kets:6 errors:0 dropped:0 overruns:0
ions:0 txqueuelen:1000
es:0 (0.0 B)  TX bytes:468 (468.0 B)
upt:19 Base address:0x2000

ncap:Local Loopback
ddr:127.0.0.1  Mask:255.0.0.0
addr: ::1/128 Scope:Host
```

About the Virtual Machines (VMs)

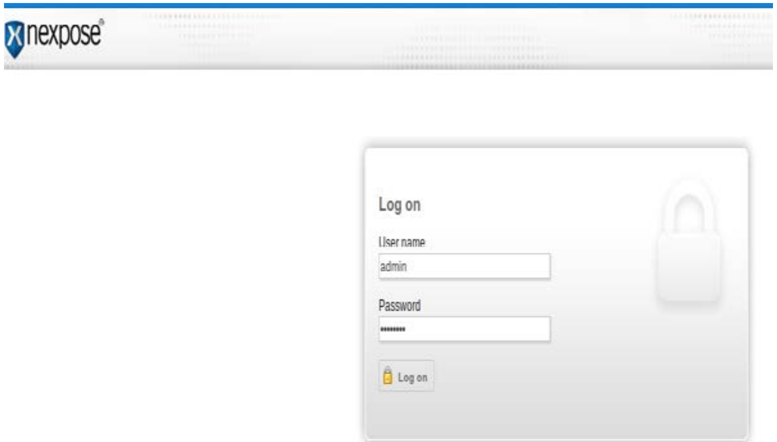
Nessus – nessus.sait230.ca

- Nessus and NeXpose vulnerability scanners;
- It will be used to check for vulnerabilities on the network services on the target machines.



Username admin

Password ********



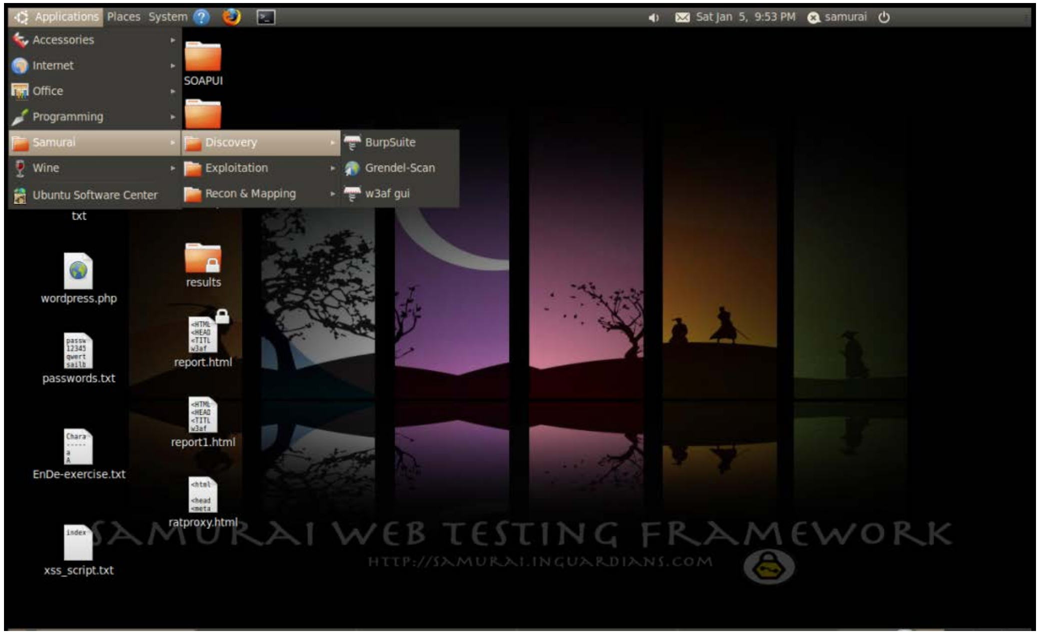
User name admin

Password ••••••••

About the Virtual Machines (VMs)

Samurai – samurai.sait230.ca

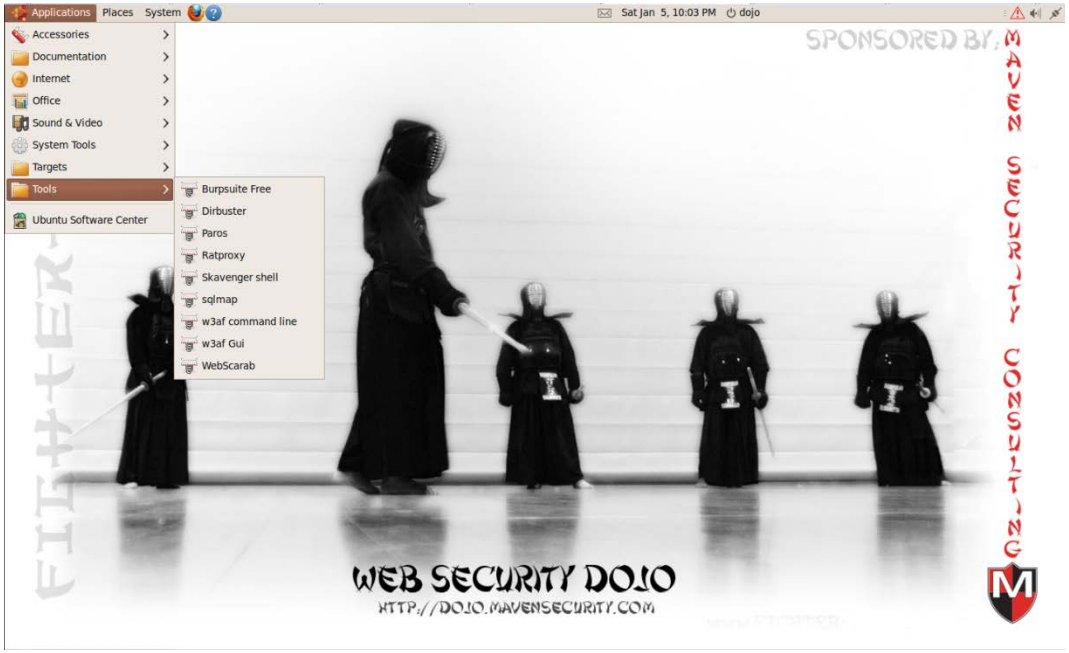
- Web Testing Frame Work;
- It has vulnerable web apps as well the tools for test them;
- Designed for web pentesting environment.



About the Virtual Machines (VMs)

Web Security Dojo – websecdojo.sait230.ca

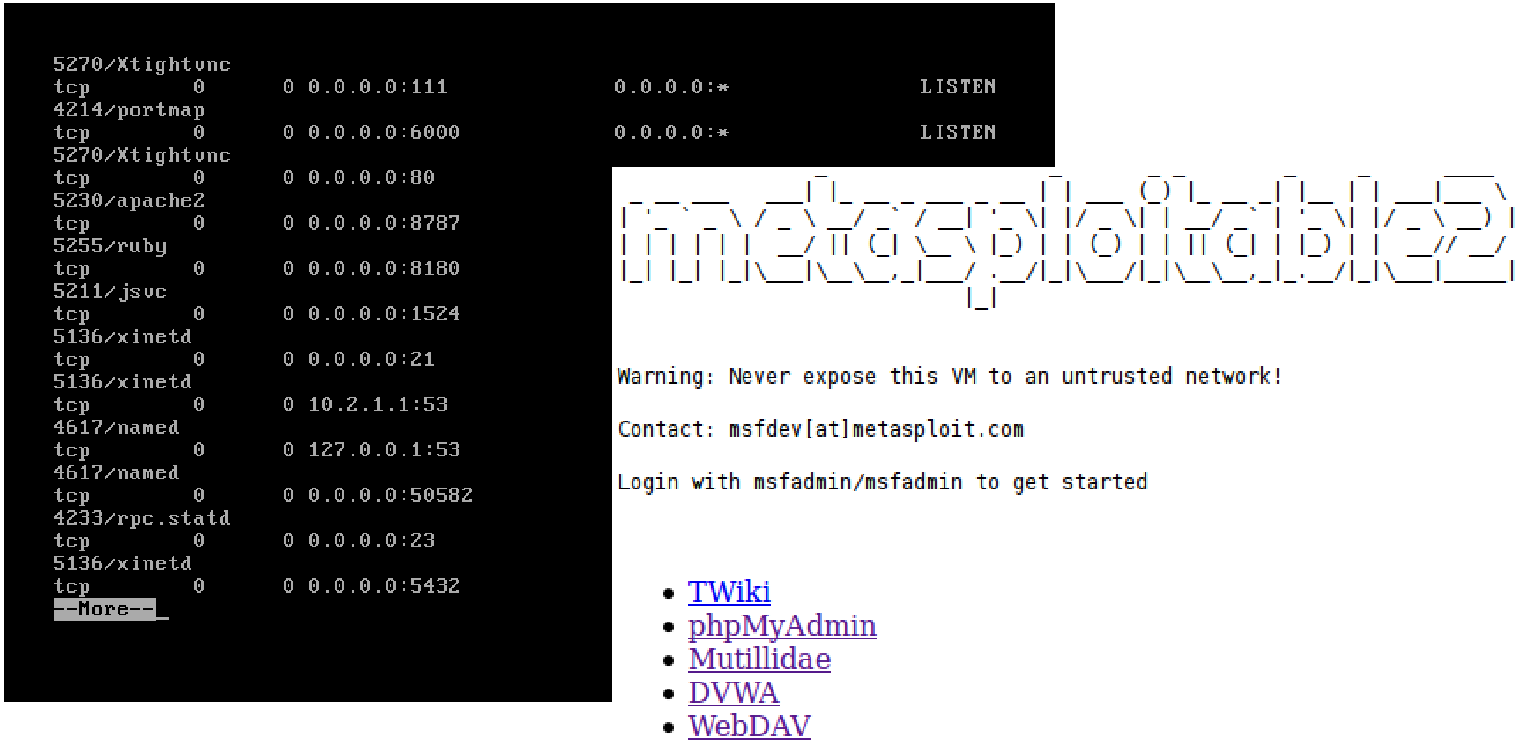
- It has vulnerable web apps as well the tools for test them;
- A preconfigured, stand-alone training environment for Web Application Security.



About the Virtual Machines (VMs)

Metasploitable – metasploitable.sait230.ca

- It has vulnerable network services and web apps for security tests;



```
5270/Xtightvnc
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
4214/portmap
tcp        0      0 0.0.0.0:6000            0.0.0.0:*               LISTEN
5270/Xtightvnc
tcp        0      0 0.0.0.0:80
5230/apache2
tcp        0      0 0.0.0.0:8787
5255/ruby
tcp        0      0 0.0.0.0:8180
5211/jsvc
tcp        0      0 0.0.0.0:1524
5136/xinetd
tcp        0      0 0.0.0.0:21
5136/xinetd
tcp        0      0 10.2.1.1:53
4617/named
tcp        0      0 127.0.0.1:53
4617/named
tcp        0      0 0.0.0.0:50582
4233/rpc.statd
tcp        0      0 0.0.0.0:23
5136/xinetd
tcp        0      0 0.0.0.0:5432
--More--_
```

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

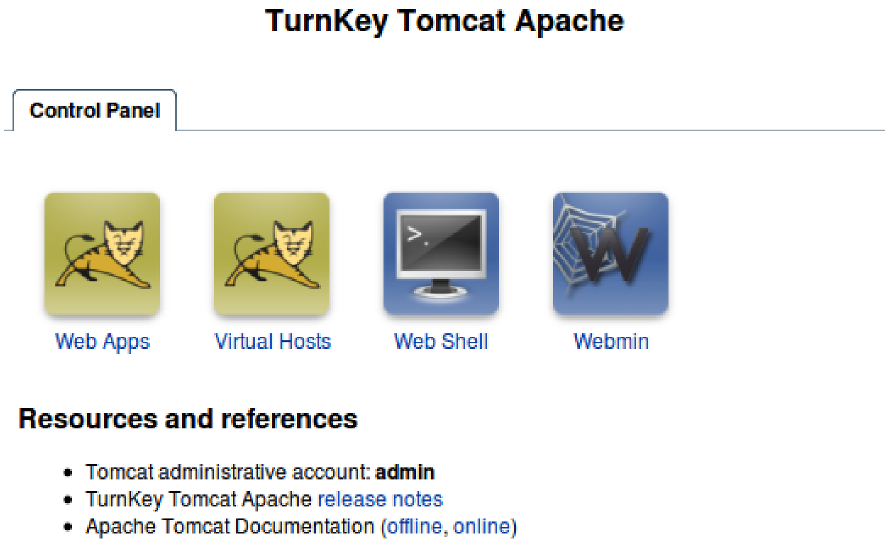
Login with msfadmin/msfadmin to get started

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

About the Virtual Machines (VMs)

Tomcat-Apache – tomcat-apache.sait230.ca

- It has Tomcat installed;
- It will be used for recon and file injection attack.



TurnKey Tomcat Apache

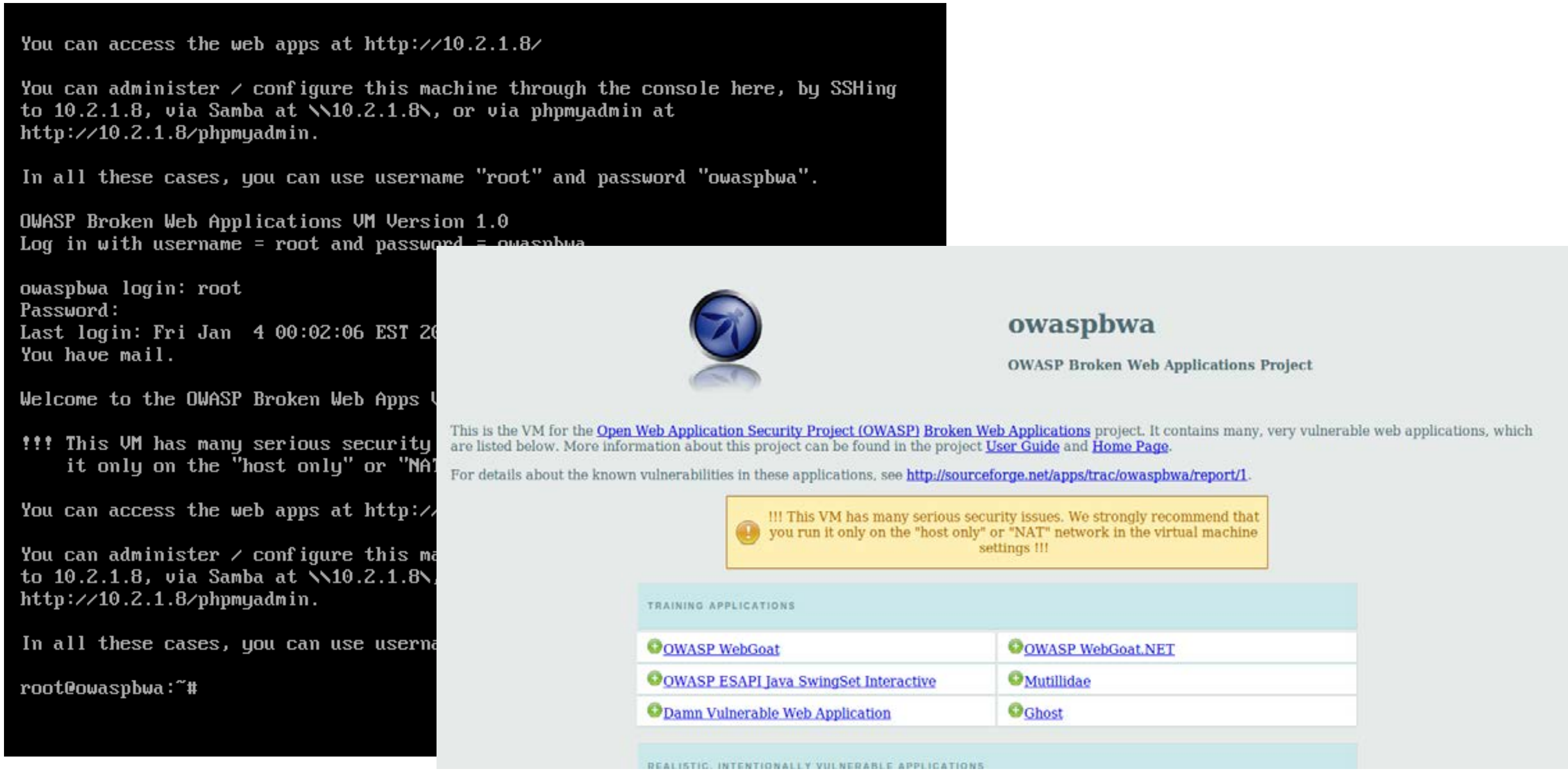
Resources and references

- Tomcat administrative account: **admin**
- TurnKey Tomcat Apache release notes
- Apache Tomcat Documentation (offline, online)

About the Virtual Machines (VMs)

OWASP Broken Web Apps – bwa.sait230.ca

- Virtual Machine running a variety of applications with known vulnerabilities.



```
You can access the web apps at http://10.2.1.8/

You can administer / configure this machine through the console here, by SSHing
to 10.2.1.8, via Samba at \\10.2.1.8\, or via phpmyadmin at
http://10.2.1.8/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

OWASP Broken Web Applications VM Version 1.0
Log in with username = root and password = owaspbwa

owaspbwa login: root
Password:
Last login: Fri Jan  4 00:02:06 EST 20
You have mail.

Welcome to the OWASP Broken Web Apps V

!!! This VM has many serious security
    it only on the "host only" or "NAT

You can access the web apps at http://

You can administer / configure this ma
to 10.2.1.8, via Samba at \\10.2.1.8\,
http://10.2.1.8/phpmyadmin.

In all these cases, you can use userna

root@owaspbwa:~#
```

owaspbwa

OWASP Broken Web Applications Project

This is the VM for the Open Web Application Security Project (OWASP) Broken Web Applications project. It contains many, very vulnerable web applications, which are listed below. More information about this project can be found in the project User Guide and Home Page.

For details about the known vulnerabilities in these applications, see http://sourceforge.net/apps/trac/owaspbwa/report/1.

!!! This VM has many serious security issues. We strongly recommend that you run it only on the "host only" or "NAT" network in the virtual machine settings !!!

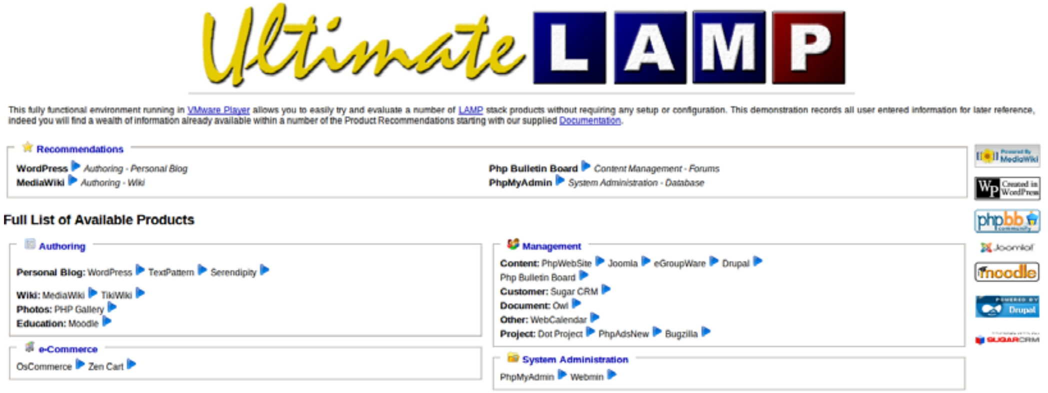
TRAINING APPLICATIONS	
OWASP WebGoat	OWASP WebGoat.NET
OWASP ESAPI Java SwingSet Interactive	Mutillidae
Damn Vulnerable Web Application	Ghost

REALISTIC, INTENTIONALLY VULNERABLE APPLICATIONS

About the Virtual Machines (VMs)

Ultimate LAMP (Linux-Apache-MySQL-PHP) – ultimatelamp.sait230.ca

- Fully functional environment allowing you to easily try and evaluate a number of LAMP apps;
- It will be used for recon, discovery and mapping phases.



This fully functional environment running in VMware Player allows you to easily try and evaluate a number of LAMP stack products without requiring any setup or configuration. This demonstration records all user entered information for later reference, indeed you will find a wealth of information already available within a number of the Product Recommendations starting with our supplied Documentation.

Recommendations

WordPress *Authoring - Personal Blog*
MediaWiki *Authoring - Wiki*
Php Bulletin Board *Content Management - Forums*
PhpMyAdmin *System Administration - Database*

Full List of Available Products

Authoring

Personal Blog: WordPress TextPattern Serendipity
Wiki: MediaWiki TikiWiki
Photos: PHP Gallery
Education: Moodle

e-Commerce

OsCommerce Zen Cart

Management

Content: PhpWebSite Joomla eGroupWare Drupal Php Bulletin Board
Customer: Sugar CRM
Document: Owl
Other: WebCalendar
Project: Dot Project PhpAdsNew Bugzilla

System Administration

PhpMyAdmin Webmin

About the Virtual Machines (VMs)

User Credentials

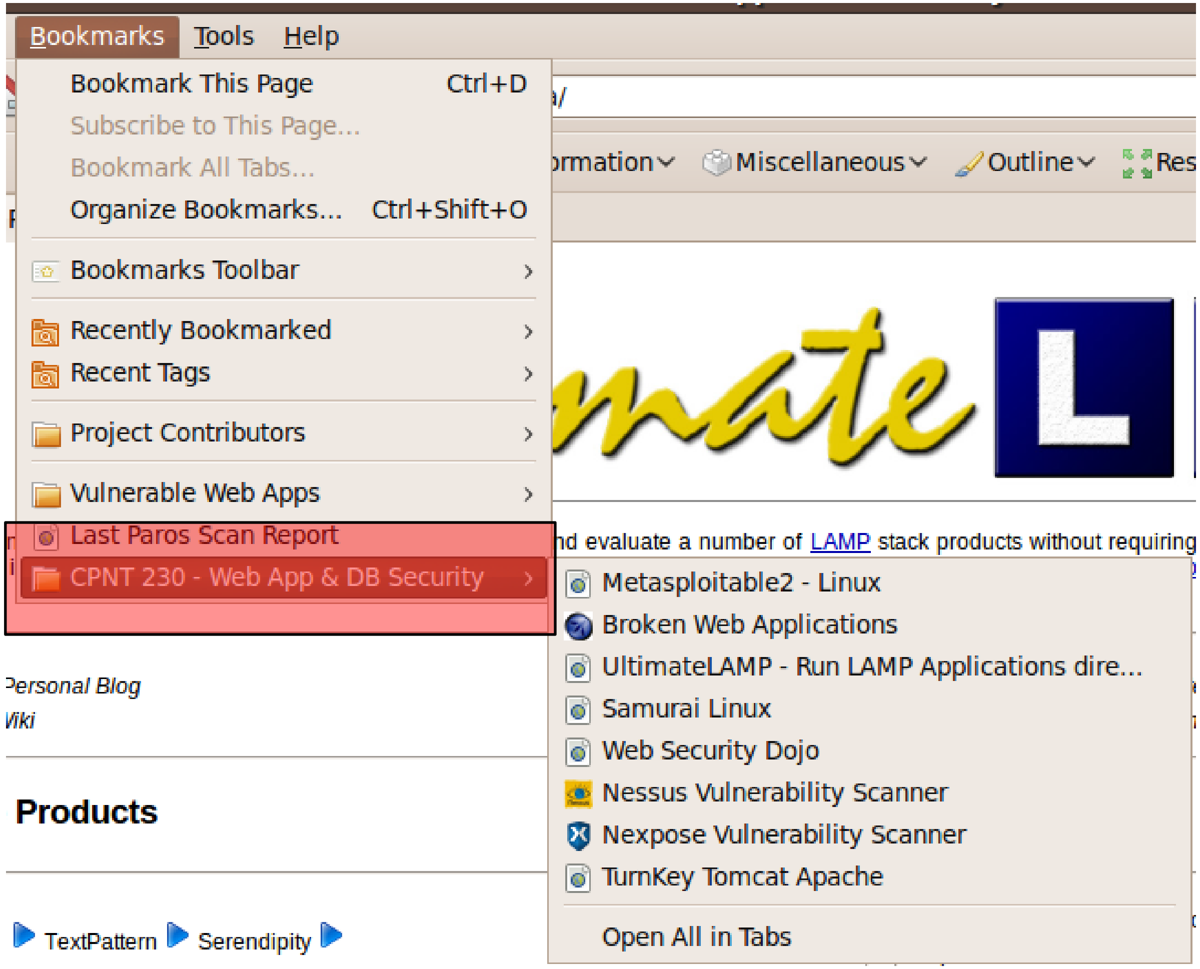
- $ users: sait, samurai - password
- # users: root, msfadmin – Password!
- Nessus / NeXpose: admin - password

Domain

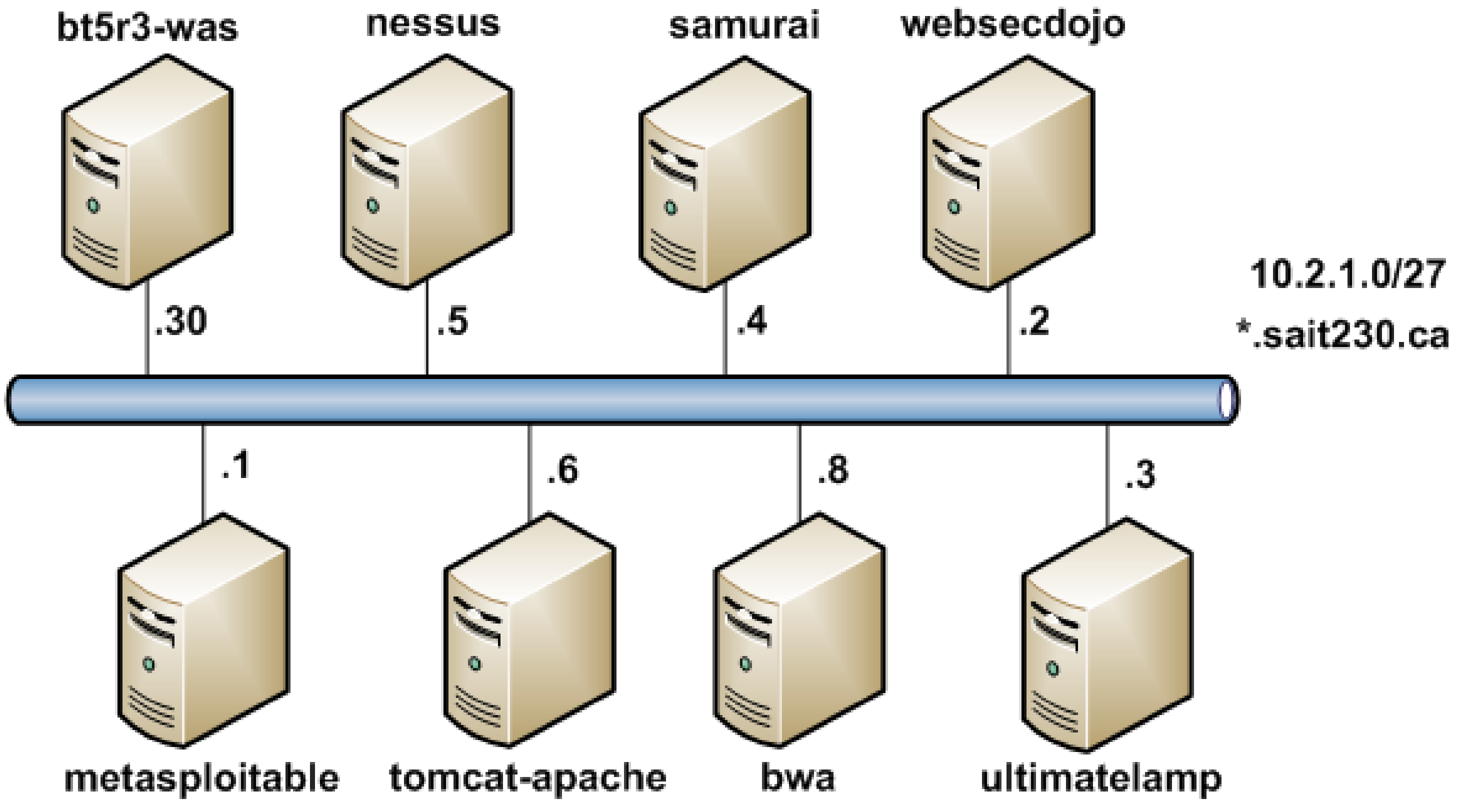
- *.sait230.ca;
- /etc/hosts

About the Virtual Machines (VMs)

Bookmarks



Lab 1 – Testing the VMs



Lab 1 – Testing the VMs

- Please copy all the VMs and place them on your desktop;
- Start the VMs selecting ***I Moved it*** to keep all the network configuration;
- Please make sure that all the VMs are reachable;
- Perform a port scan from bt5r3-was against all the machines to check:
  - OS;
  - Open Ports;
  - Service Version.

Questions