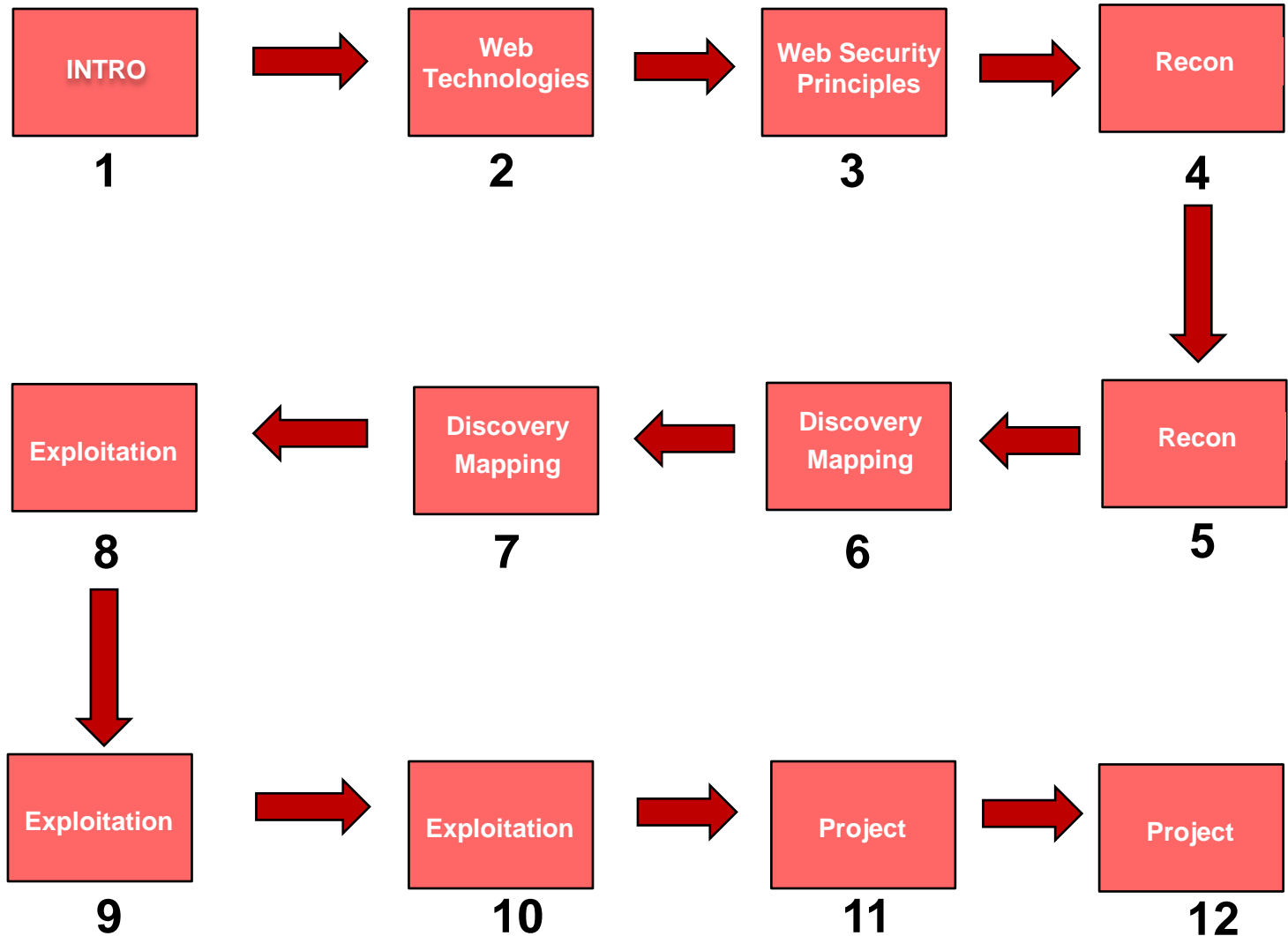


Web App & Data Base Security

Mapping

Web App & Data Base Security



Agenda

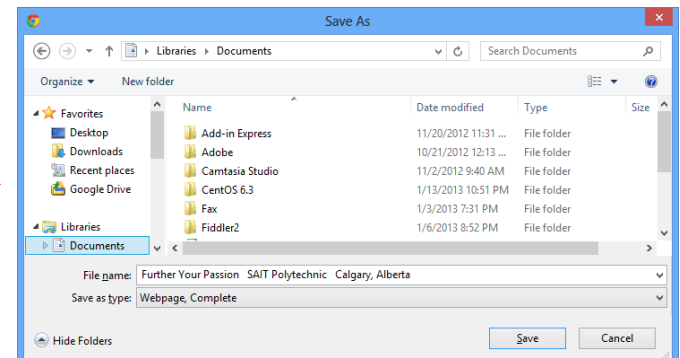
- Spidering;
- Robots;
- Proxy Architecture;
- WebScarab;
- Burp Suite;
- Vulnerability Scanning with Nessus.
- Lab 1: Spidering a Website;
- Lab 2: Discovering Vulnerabilities on web services.

Spidering the Target Web Site

- 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
→



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 Methods

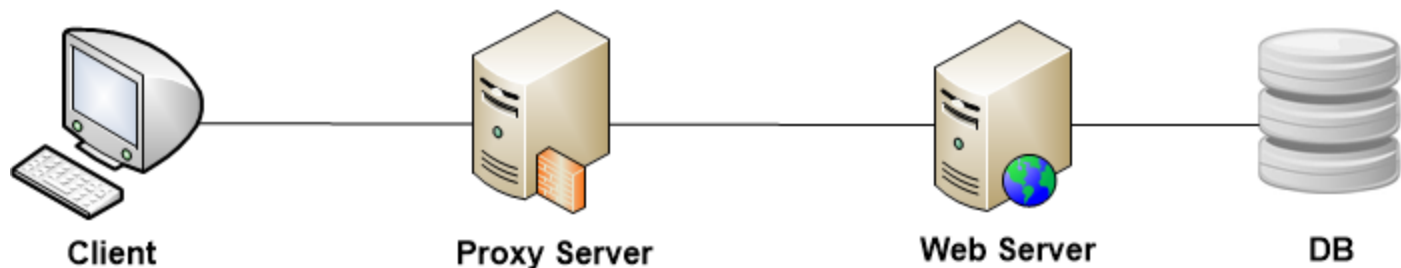
- Manual and automated spidering;
- Manual browsing the site and save each page;
- May be necessary if automated scanning fails;
- Automated scans may fail because the site is complex or has issues;
- Automated tools:
 - Wget;
 - WebScarab;
 - Burp Suite;
 - Paros.

Robot Control – Robot.txt

- 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.

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.



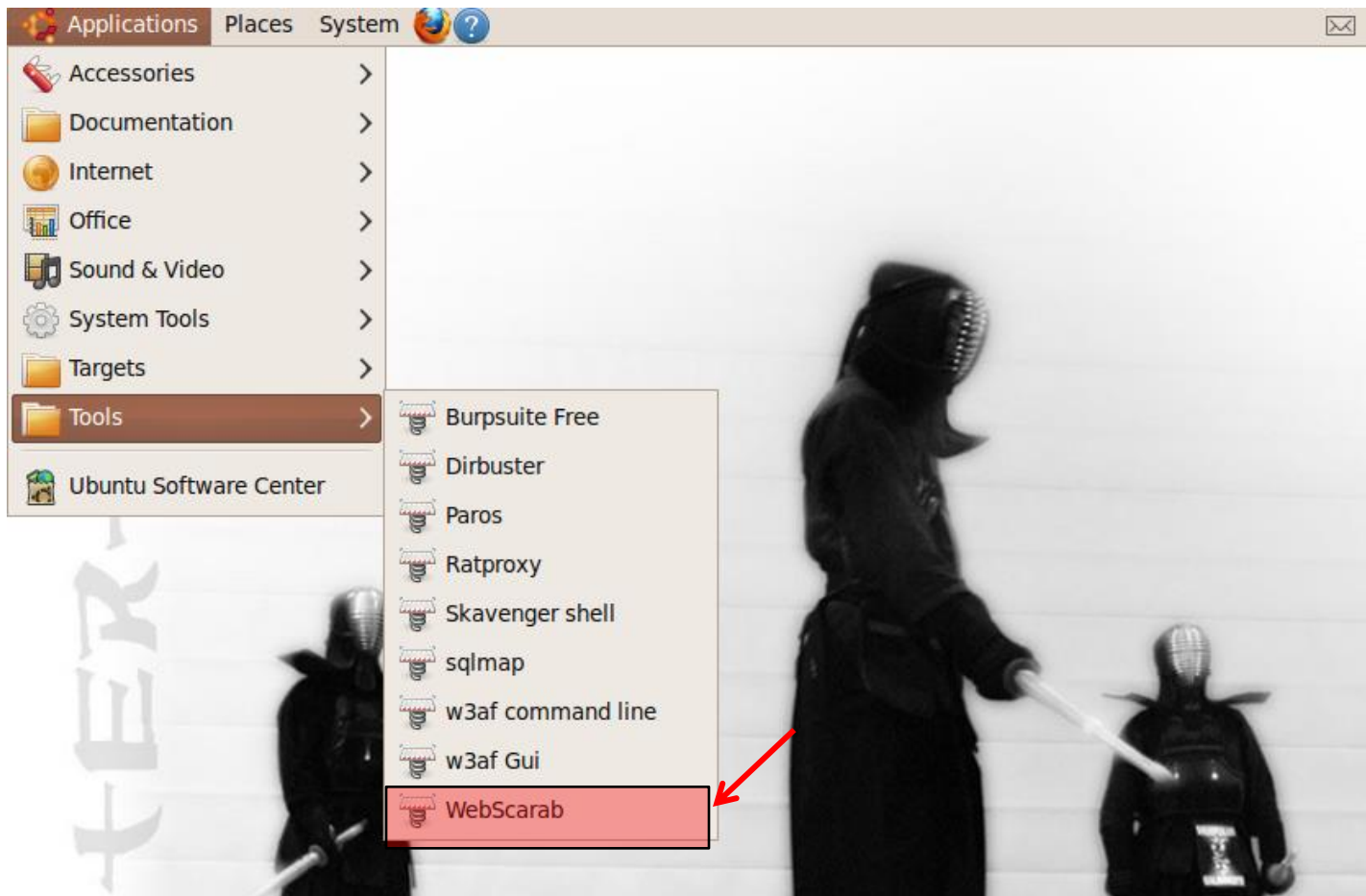
WebScarab

- 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

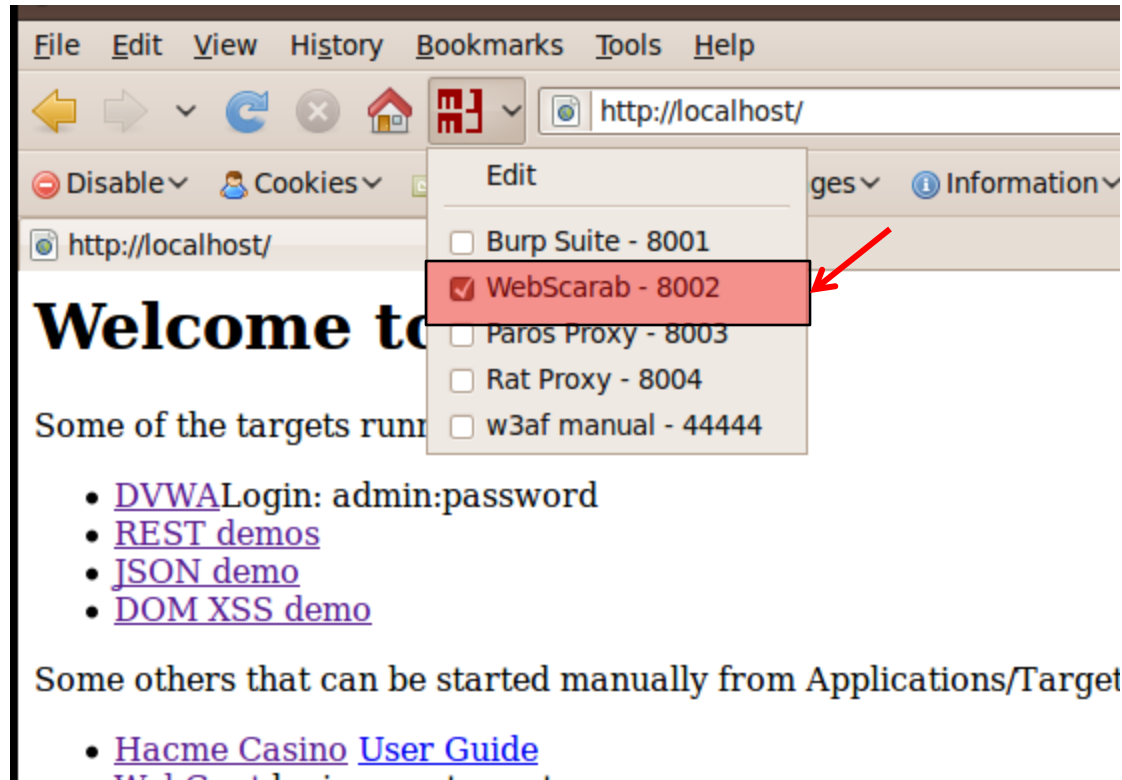
Step 1: Starting the intercepting proxy



Spidering a Website - WebScarab

Mapping

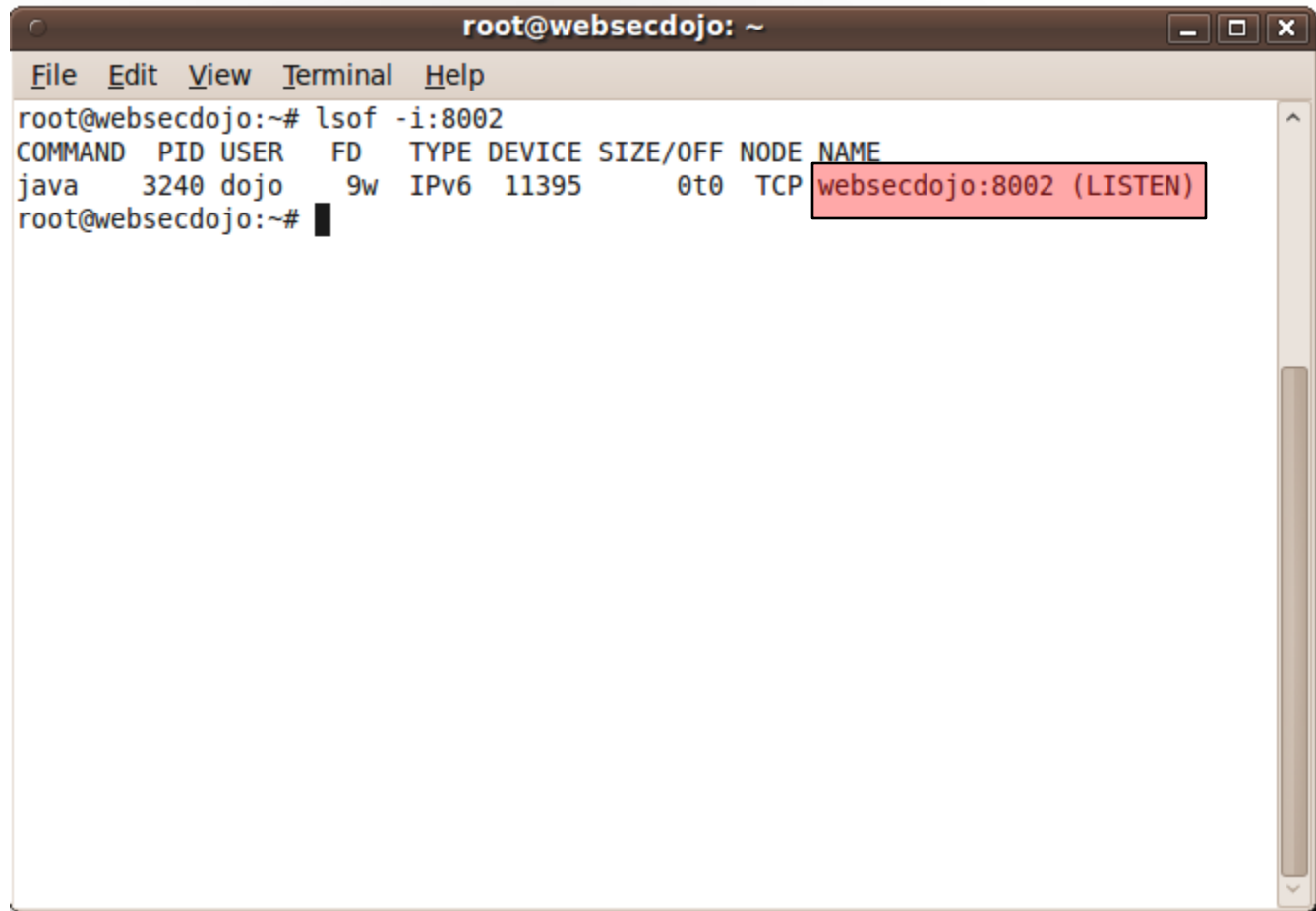
Step 2: Selecting the proxy – WebScarab:8002



Spidering a Website - WebScarab

Step 2: Selecting the proxy – WebScarab:8002

Mapping



A terminal window titled 'root@websecdojo: ~' showing the command 'lsof -i:8002' and its output. A red arrow points to the 'COMMAND' column of the output table. The output table has columns: COMMAND, PID, USER, FD, TYPE, DEVICE, SIZE/OFF, NODE, and NAME. The output shows a single entry for 'java' with PID 3240, user 'dojo', listening on IPv6 port 11395. The NAME column shows 'websecdojo:8002 (LISTEN)' which is highlighted with a red box.

```
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

Step 3: Browsing the target web app

Mapping

The screenshot shows a web browser window with the address bar set to `http://metasploitable.sait230.ca/`. The browser displays the Metasploit logo and a warning message: "Warning: Never expose this VM to an untrusted network." Below the warning, it provides contact information: "Contact: msfdev[at]metasploit.com" and login instructions: "Login with msfadmin/msfadmin to get started". A list of links is provided: [TWiki](#), [phpMyAdmin](#), [Mutillidae](#), [DVWA](#), and [WebDAV](#).

Overlaid on the browser is the WebScarab application window. The "Spider" tab is selected, and the "Tree Selection filter" is set to "conversation list". A red arrow points to the "Tree Selection filter" dropdown. The "conversation list" table shows a single entry for the URL `http://metasploitable.sait230.ca:80/` with a status of "200 OK".

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

The status bar at the bottom of the WebScarab window indicates "Used 4.93 of 63.56MB".

Spidering a Website - WebScarab

Step 3: Browsing the target web app

Mapping

TWiki Reference Manual

This page contains all documentation topics. **Doubleclick anywhere** to return to the top.

- [TWiki System Requirements](#)
 - [Server Requirements](#)
 - [Client Requirements](#)
 - [Known Issues](#)
- [TWiki Installation Guide](#)
 - [Standard Installation](#)
 - [Step 1: Create & Configure](#)
 - [Step 1 for Non-Root Admin](#)
 - [Step 2: Set File Permissions](#)
 - [Step 3: Set the Main Configuration](#)
 - [Step 4: Configure Site-Wide Settings](#)
 - [Step 5: Finish Up from Your Web Browser](#)
 - [Additional Server-Level Options](#)
 - [Enabling Authentication of Users](#)
 - [TWiki File System Info](#)
- [Windows Install Cookbook](#)
 - [Introduction](#)
 - [Recent updates](#)

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

WebScarab is saving all the content accessed.

Spidering a Website - WebScarab

Step 4: WebScarab Console - Summary

Mapping

The screenshot shows the WebScarab application window. The 'Summary' tab is selected, displaying a 'Tree Selection filters conversation list' on the left and a table of requests on the right. A red arrow points to the 'Spider tree' in the left pane.

Tree Selection filters conversation list

- ☐ http://metasploitable.sait230.ca:80/
 - ☐ p/
 - ☐ twiki/
 - ☐ TWikiDocumentation.html

Spider tree

- Show scripts
- Show comments

Request List

ID	Date	Method	Host	Path	Parameters	Status	Other
11	2013/01/19 18:30:30	GET	http://metasploitable.sait230.ca:80	/p/pub/1cn/txt.gif		404 Not F...	Prox...
10	2013/01/19 18:30:30	GET	http://metasploitable.sait230.ca:80	/p/pub/1cn/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...

Used 12.97 of 63.56MB

Spidering a Website - WebScarab

Step 4: WebScarab Console - Summary

Mapping

The screenshot shows the WebScarab application window. The 'Summary' tab is selected, displaying a 'Tree Selection filters conversation list'. A red box highlights the discovered URLs, including [TWiki](#), [phpMyAdmin](#), [Mutillidae](#), [DVWA](#), and [WebDAV](#). A red arrow points from this box to the 'Tree Selection filters conversation list'.

Warning: Never expose this VM to an untrusted network.

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

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
74	2013/01/19 18:36:32	GET	http://metasploitable.sait230.ca:80/	/mutillidae/images/owasp-logo-400-300.png		200 OK
73	2013/01/19 18:36:17	GET	http://metasploitable.sait230.ca:80/	/mutillidae/index.php	?page=ar...	200 OK
72	2013/01/19 18:36:17	GET	http://metasploitable.sait230.ca:80/	/mutillidae/index.php	?page=ad...	200 OK
71	2013/01/19 18:36:17	GET	http://metasploitable.sait230.ca:80/	/mutillidae/index.php	?do=toggl...	302 Found
70	2013/01/19 18:36:17	GET	http://metasploitable.sait230.ca:80/	/mutillidae/index.php	?do=toggl...	302 Found
69	2013/01/19 18:36:17	GET	http://metasploitable.sait230.ca:80/	/mutillidae/index.php		200 OK
68	2013/01/19 18:36:17	GET	http://metasploitable.sait230.ca:80/	/mutillidae/images/youtube_256_256.png		200 OK
67	2013/01/19 18:36:17	GET	http://metasploitable.sait230.ca:80/	/mutillidae/images/toad-for-mysql-77-80.jpg		200 OK
66	2013/01/19 18:36:17	GET	http://metasploitable.sait230.ca:80/	/mutillidae/images/samurai-wtf-logo-320-214.jpeg		200 OK
65	2013/01/19 18:36:17	GET	http://metasploitable.sait230.ca:80/	/mutillidae/images/php-mysql-logo-176-200.jpeg		200 OK
64	2013/01/19 18:36:17	GET	http://metasploitable.sait230.ca:80/	/mutillidae/images/bui_eclipse_pos_logo_fc_med.jpg		200 OK
63	2013/01/19 18:36:17	GET	http://metasploitable.sait230.ca:80/	/mutillidae/images/coykillericon.png		200 OK
62	2013/01/19 18:36:17	GET	http://metasploitable.sait230.ca:80/	/mutillidae/images/backtrack-4-r2-logo-90-69.png		200 OK
61	2013/01/19 18:36:17	GET	http://metasploitable.sait230.ca:80/	/mutillidae/images/backBanner3x_final_print.jpg		200 OK

Used 14.37 of 63.56MB

Spidering a Website - WGET

- 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 26
```

Burp Suite

- 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

- 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

The screenshot shows the Burp Suite v1.3 interface. The browser window at the top displays the URL `http://metasploitable.sait230.ca/`. The Burp Suite window is open, showing the 'site map' tab. The site map displays a tree structure of the website's resources, including folders like `/`, `dav`, `dwa`, `mutillidae`, `phpMyAdmin`, and `twiki`. A context menu is open over the `http://metasploitable.sait230.ca/` entry, with the 'spider this host' option highlighted by a red arrow. To the left of the site map, a pink box contains a list of items to be mapped:

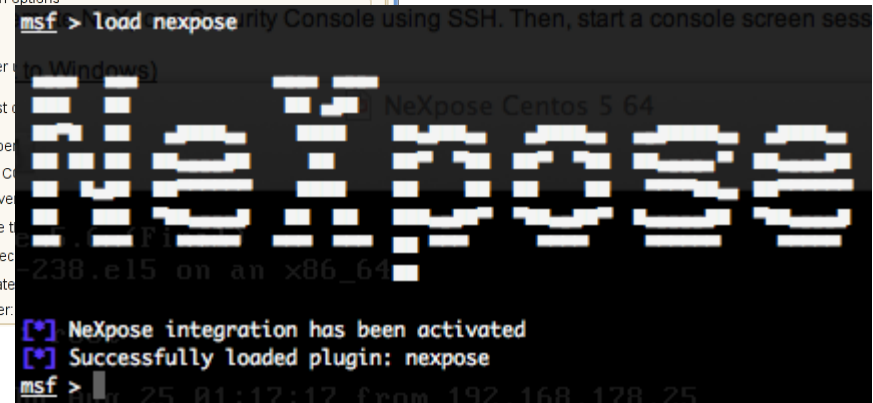
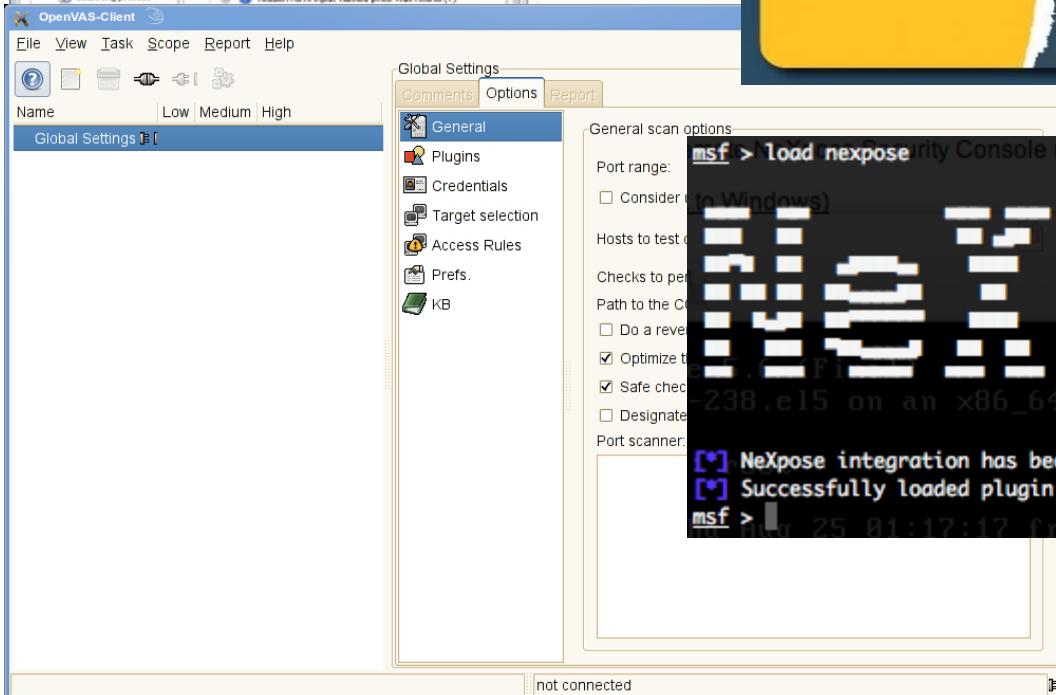
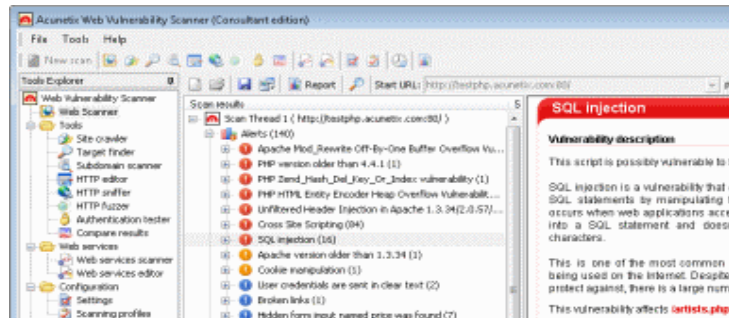
- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

The bottom right pane shows the 'request' tab, displaying the HTTP response for the selected URL. The response status is '200 OK' and the content type is 'text/html'. The response body shows the beginning of an HTML document with the title 'Metasploitable2 - Linux'.

Vulnerability Identification

Vulnerability Scanners

Discovering



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

Nessus Architecture

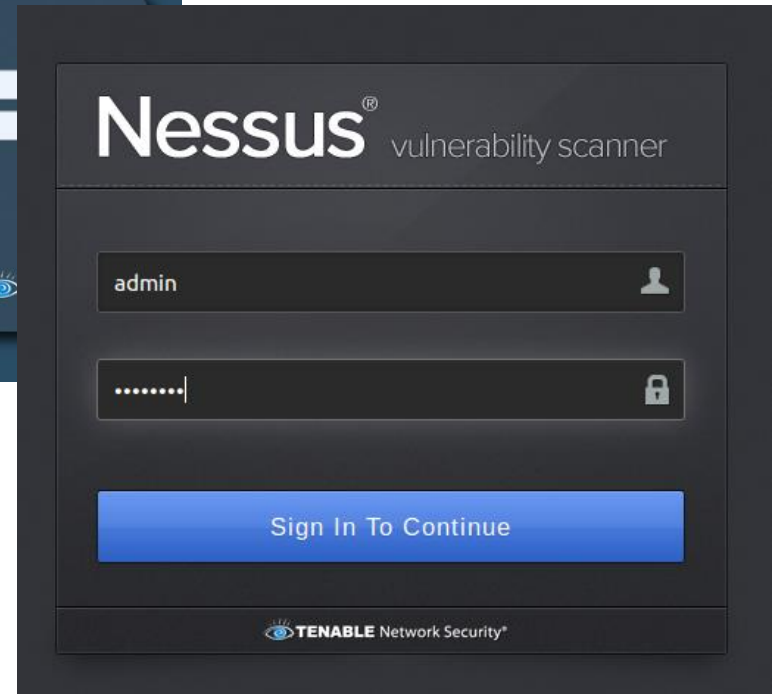
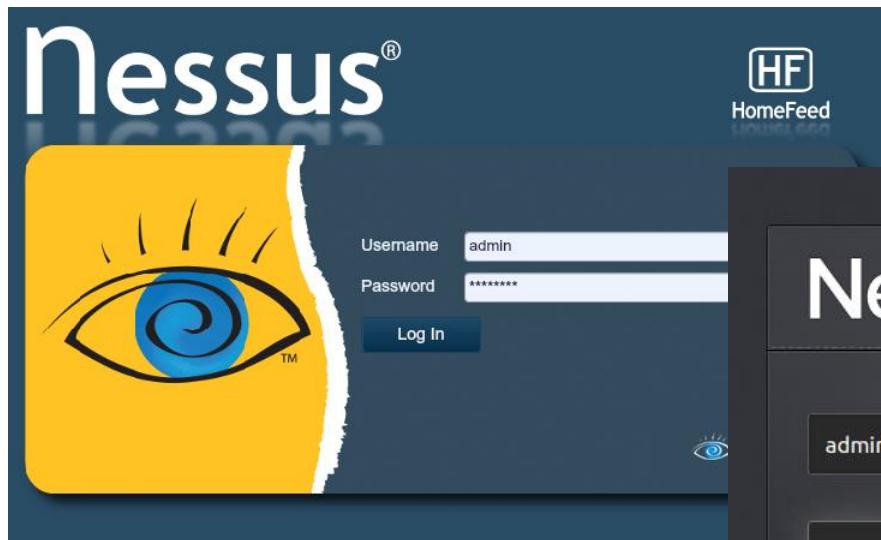
Discovering



https://ip_address:8834

Vulnerability Scanning - Nessus

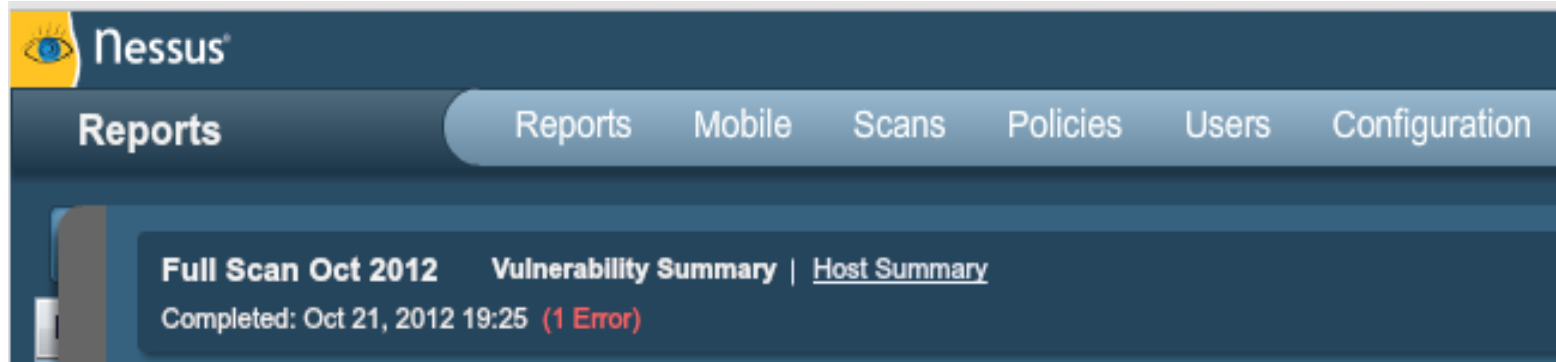
<https://192.168.X.XX:8834/>



Discovering

Vulnerability Scanning - Nessus

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



Discovering

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

Vulnerability Scanning - Nessus

Discovering

Scans

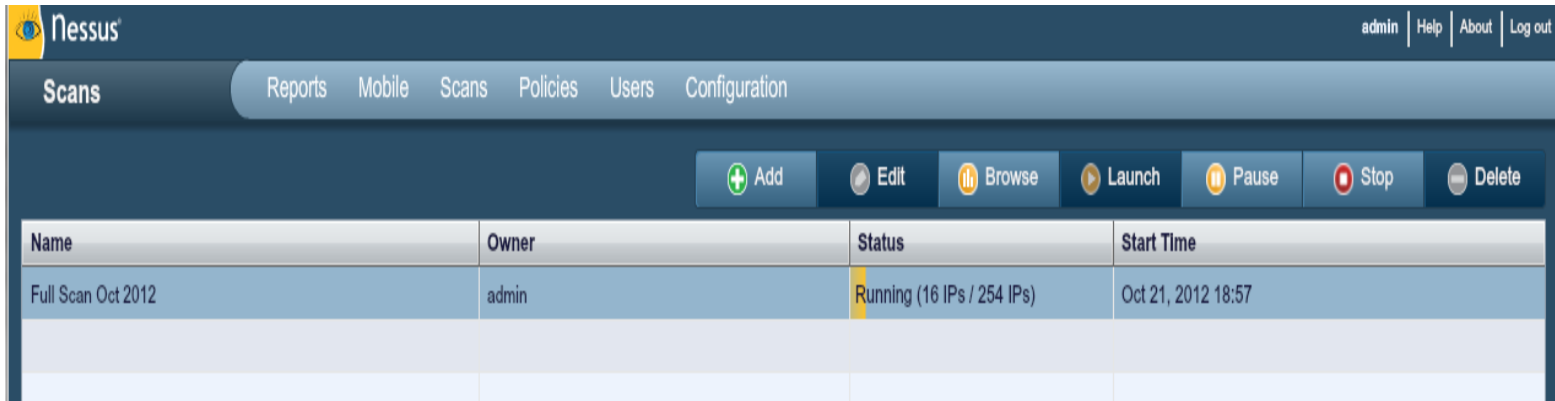
The screenshot displays the Nessus web interface for configuring a scan. The top navigation bar includes links for Reports, Mobile, Scans, Policies, Users, and Configuration. The main content area is titled 'Scans' and features a '+ Add Scan' button. The configuration form includes the following fields:

- Name:** Full Scan Oct 2012
- Type:** Run Now (dropdown menu)
- Policy:** Internal Network Scan (dropdown menu)
- Scan Targets:** 192.168.1.0/24 (text area)
- Targets File:** (text input field with a 'Browse...' button)

At the bottom right, there are 'Cancel' and 'Launch Scan' buttons.

Vulnerability Scanning - Nessus

Scanning



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

Results

Upload Report Browse Compare Download Delete		
Name	Status	Last Updated
Full Scan Oct 2012	Completed	Oct 21, 2012 19:25
Mestasploitable Server oct-2012	Completed	Oct 21, 2012 11:34

Filters No Filters Add Filter Clear Filters				
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	vstftpd 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

Discovering

Vulnerability Scanning - Nessus

Results

Discovering

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	Host	Port
46882	2	192.168.1.83	6667 / tcp
10380	1		
25216	1		
32314	1		
51988	1		
55523	1		
61708	1		
61730	1		
62062	1		
62369	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		

← 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/2010/06/12>
<http://seclists.org/fulldisclosure/2010/06/12>
<http://www.unrealircd.com/txt/unrealsecadvisory20100612.txt>

Risk Factor: Critical

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



Buttons: Add, Export, Copy, Edit, Delete

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

+ Add Policy

General

Credentials

Plugins

Preferences

Basic

Name

Visibility

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

Performance

Max Checks Per Host

Max Hosts Per Scan

Network Receive Timeout (seconds)

Max Simultaneous TCP Sessions Per Host

Max Simultaneous TCP Sessions Per Scan

Vulnerability Scanning - Nessus

Discovering

Policies

The screenshot shows the Nessus web interface for configuring a policy. The top navigation bar includes 'Policies', 'Reports', 'Mobile', 'Scans', 'Policies', 'Users', and 'Configuration'. The left sidebar has a menu with 'General', 'Credentials', 'Plugins', and 'Preferences'. The main content area is titled 'Add Policy' and shows the configuration for 'SSH settings'.

Nessus adm

Policies Reports Mobile Scans Policies Users Configuration

+ Add Policy

Credential Type: SSH settings

SSH user name : msfadmin

SSH password (unsafe) : *****

SSH public key to use : Browse...

SSH private key to use : Browse...

Passphrase for SSH key :

Elevate privileges with : Nothing

su login :

Escalation account : root

Escalation password :

SSH known_hosts file : Browse...

Preferred SSH port : 22

Client version : OpenSSH_5.0

Vulnerability Scanning - Nessus

Discovering

Policies

The screenshot displays the Nessus web interface for managing policies. The top navigation bar includes links for 'admin', 'Help', 'About', and 'Log'. Below this, a secondary navigation bar shows 'Policies', 'Reports', 'Mobile', 'Scans', 'Policies', 'Users', and 'Configuration'. The left sidebar contains a '+ Add Policy' button and a list of policy sections: 'General', 'Credentials', 'Plugins', and 'Preferences'. The main content area is titled 'Policies' and features a filter bar with 'Filters' and 'No Filters' tabs. A filter dropdown is set to 'All', and a search bar contains 'Bugtraq ID' with the operator 'is equal to'. Below the filter bar, there are two columns of plugins. The 'Families' column lists various security checks and categories, with 'CISCO' currently selected. The 'Plugins' column lists specific vulnerability checks, each with a green status icon. The interface is designed for configuring and managing vulnerability scanning policies.

Vulnerability Scanning - Nessus

Discovering

Policies

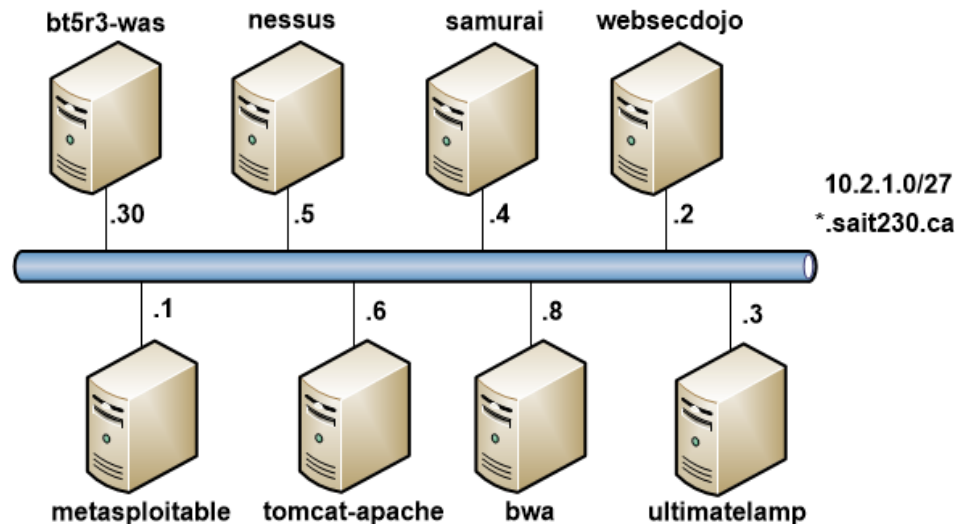
The screenshot shows the Nessus web interface. The top navigation bar includes 'Reports', 'Mobile', 'Scans', 'Policies', 'Users', and 'Configuration'. The 'Policies' tab is selected. On the left, there is a sidebar with 'Add Policy' and a list of policy sections: 'General', 'Credentials', 'Plugins', and 'Preferences'. The 'Plugins' section is active, showing the 'ADSI Settings' plugin selected in a dropdown menu. The main area contains a form for configuring the plugin, with fields for 'Domain Controller', 'Domain', 'Domain Username', and 'Domain Password' repeated five times.

Field	Value
Domain Controller 1:	
Domain 1:	
Domain Username 1:	
Domain Password 1:	
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

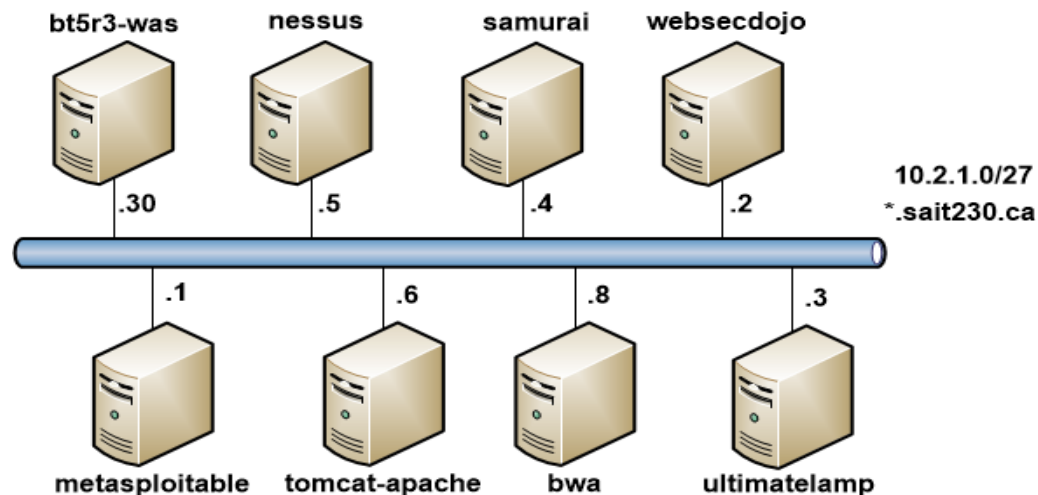
Mapping

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



Project – Phase 2: Discovery

- 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?

Questions

