

SEC520

Penetration Testing (continued): Exploiting Vulnerabilities



Today's Objectives

Vulnerability Testing: (Lab3 - part2)

- Purpose / Warning
- Techniques and Tools:
 - **Nessus**
 - **Metasploit**



Vulnerability Testing

Purpose of Vulnerability Testing:

- This stage becomes the “collection point” for all information collected in the **reconnaissance**, **scanning**, and **enumeration** stages.
- We can now research what OS and running processes (port #s) is the weakest link to gain access into the system.
- In order to save time, applications or frameworks have been created that contain a **database** of known exploits, and can automatically, and exploit the server' s weakness.



Vulnerability Testing

Warning!

- To date, any reconnaissance activity is considered to be “safe” for the penetration tester.
- The tester will “cross the line” when they start to **scan ports**, or **use utilities that exploit vulnerabilities** on a server to gain unauthorized access.
- If the tester does **NOT** have written permission, and possibly a signed “Rules of Engagement” contract prior to scanning / vulnerability testing, they may be subject to **legal action or account suspension from their ISP!**



Vulnerability Testing

Vulnerability Testing Tools:

- There are many applications can can be used for Vulnerability testing (both open-source and proprietary).
- In lab #3, we will be using two open-source applications:
 - **Nessus** (local site exploitation)
 - **Metasploit** (remote exploitation)

Vulnerability Testing



Testing Local Vulnerabilities - Nessus:

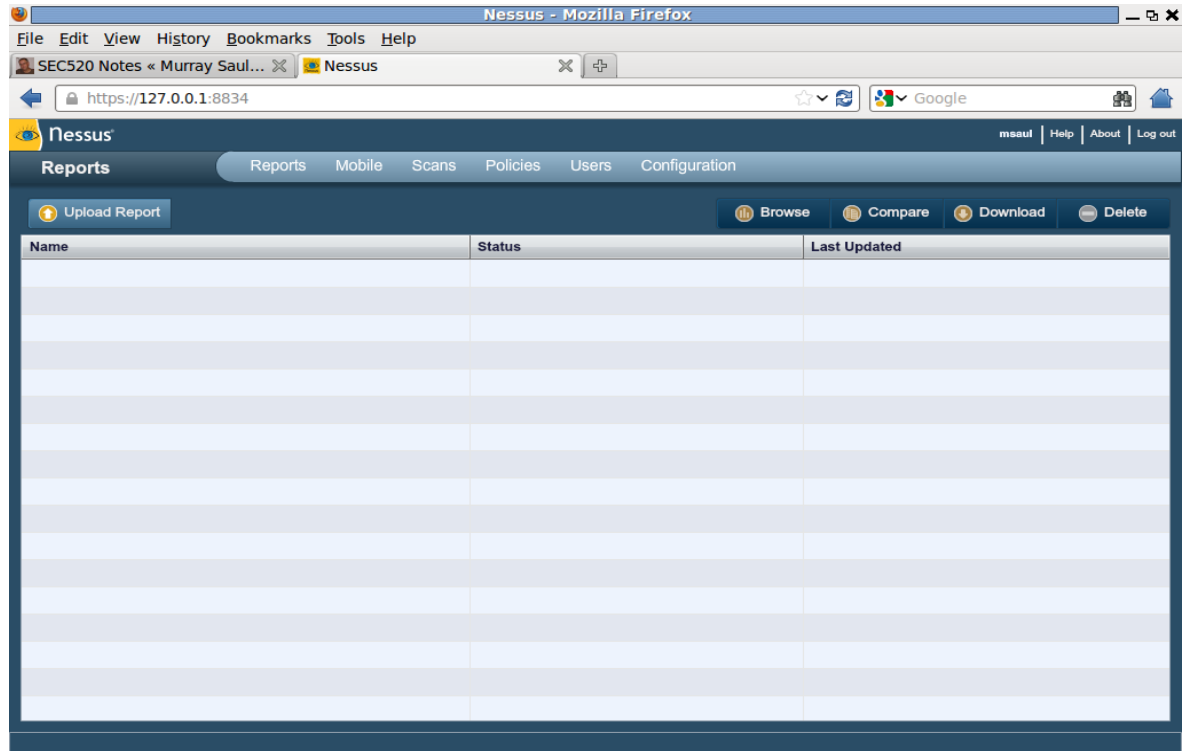
- This application is *open-source*.
- Tester must be **connected to network locally**.
- Nessus can perform *scanning & enumeration*, and *provide a report that listing vulnerable ports for exploitation* from a database of vulnerabilities.
- Full scans may increase the chances of detection from target network's IDS.
- Usually, a longer learning curve is associated with this application including the *NASAL* scripting tool.

Vulnerability Testing

In **Nessus**, you create policies (classifications) for penetration testing.

When you perform the scan, it performs exploits in order to identify vulnerabilities.

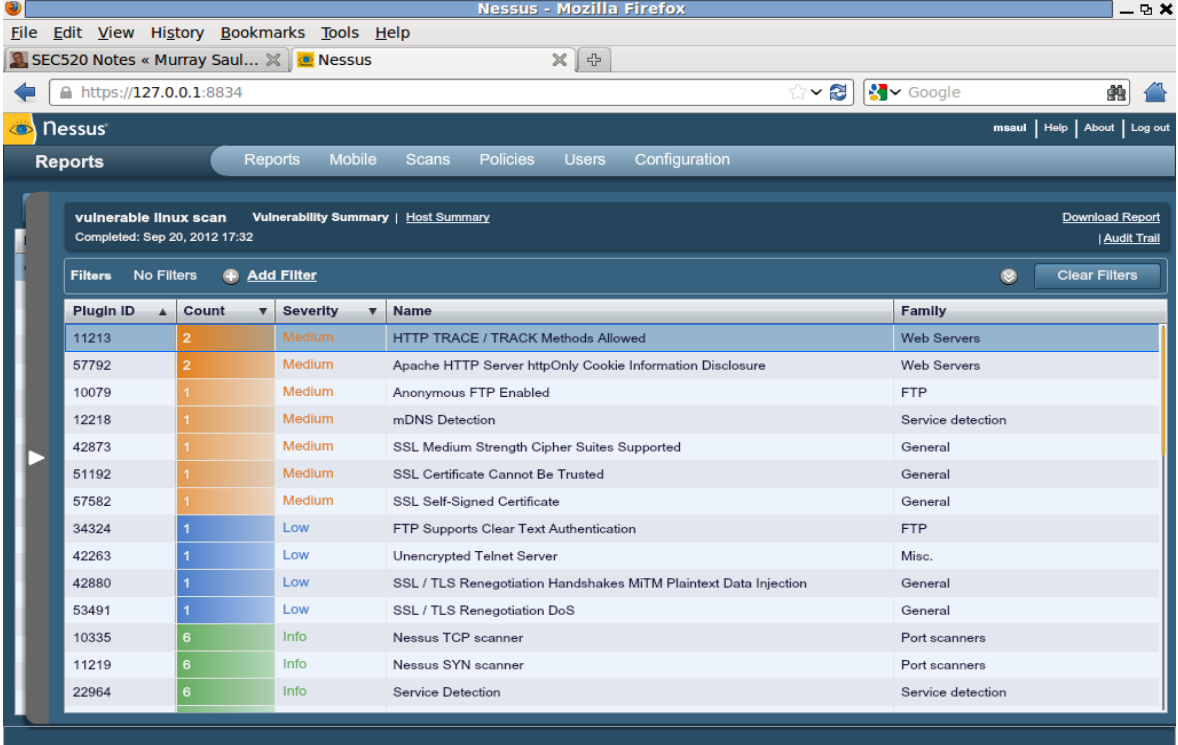
Scanning profiles can be saved for later use...



Vulnerability Testing

Reports can be generated for different servers (of different aspects of penetration testing).

Reports rank the vulnerabilities by **high**, **medium**, and **low** threats...



The screenshot shows the Nessus web interface in a Mozilla Firefox browser. The address bar displays 'https://127.0.0.1:8834'. The interface includes a navigation menu with 'Reports', 'Mobile', 'Scans', 'Policies', 'Users', and 'Configuration'. The main content area shows a 'vulnerable linux scan' report, completed on Sep 20, 2012 at 17:32. A table lists various vulnerabilities with columns for Plugin ID, Count, Severity, Name, and Family.

Plugin ID	Count	Severity	Name	Family
11213	2	Medium	HTTP TRACE / TRACK Methods Allowed	Web Servers
57792	2	Medium	Apache HTTP Server httpOnly Cookie Information Disclosure	Web Servers
10079	1	Medium	Anonymous FTP Enabled	FTP
12218	1	Medium	mDNS Detection	Service detection
42873	1	Medium	SSL Medium Strength Cipher Suites Supported	General
51192	1	Medium	SSL Certificate Cannot Be Trusted	General
57582	1	Medium	SSL Self-Signed Certificate	General
34324	1	Low	FTP Supports Clear Text Authentication	FTP
42263	1	Low	Unencrypted Telnet Server	Misc.
42880	1	Low	SSL / TLS Renegotiation Handshakes MITM Plaintext Data Injection	General
53491	1	Low	SSL / TLS Renegotiation DoS	General
10335	6	Info	Nessus TCP scanner	Port scanners
11219	6	Info	Nessus SYN scanner	Port scanners
22964	6	Info	Service Detection	Service detection



Vulnerability Testing

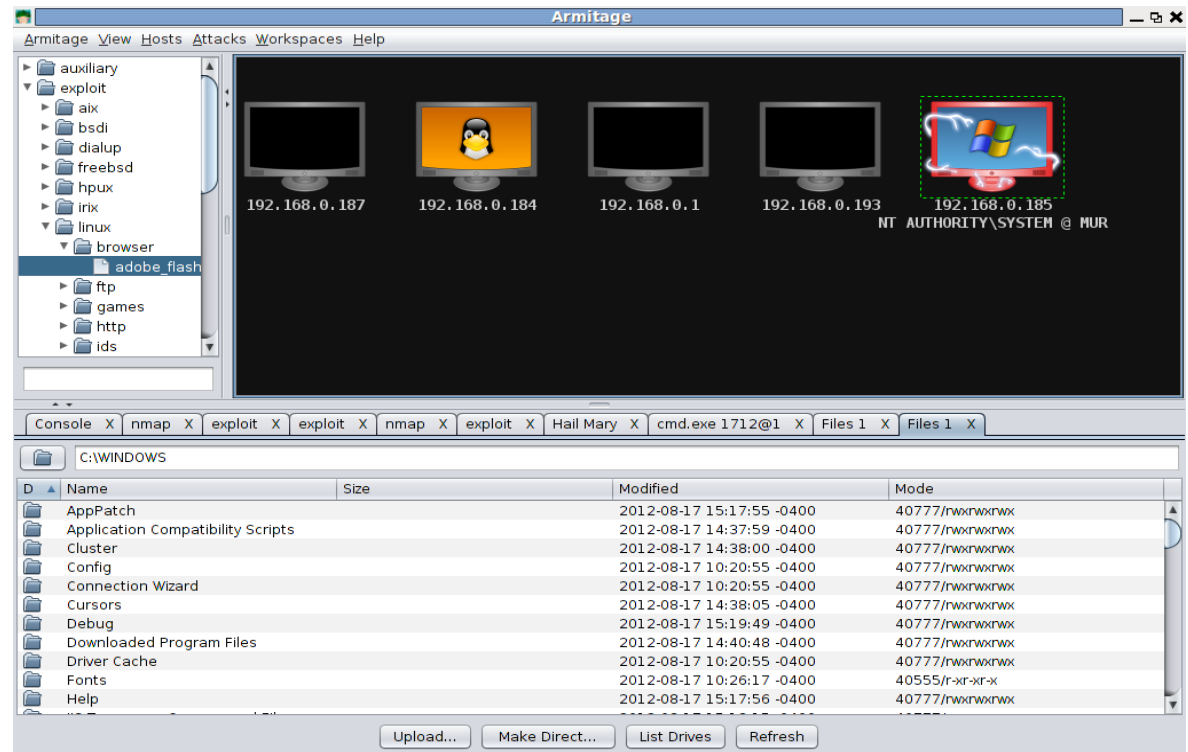
Testing Remote Vulnerabilities - Metasploit:

- This is an *open-source* application.
- This is referred to as a “**framework**” that supports many **plugins** for up-to-date exploits.
- This application can be used from **remote** networks.
- Also has ability to perform *scanning & enumeration*, and *flagging vulnerabilities* for exploitation.

Vulnerability Testing

Metasploit uses a database of exploits, and sends a package to attempt gaining access to the system.

Once the system has been **“cracked”** (Refer to the icon in the diagram!), the penetration tester can take screenshots, browse files, and even gain access to a command prompt!





Lab Time

Continue Working on:

Lab 3: Scanning, Enumeration & Vulnerability Testing
(Investigations 4 & 5)