

Audit de Sécurité Technique

Practical Lab Discovery & Exploitation

Abraham Rubinstein & Jean-Marc Bost

abraham.rubinstein@heig-vd.ch & jean-marc.bost@heig-vd.ch

Discovery and Exploitation (Lab1 & Lab2)

- This lab is divided in 2 parts:
 - Machine **discovery** and **service fingerprinting** (03.10)
 - Vulnerability **exploitation** (10.10)



Lab1 - Discovery

Machine discovery and services fingerprinting

- The goal of this lab
 - Get familiar with network recon techniques (nmap, vulnerability scanning, services discovering, exploit-db search)
 - Hands-on introduction to ethical hacking methods and CTF (Capture the Flag) methodologies
 - Get familiar with a reporting tool to keep trace of your findings
- Objective
 - Discover all running machines on the 10.10.40.0/24 network
 - Discover all running services and everything about their versions
 - Find out vulnerabilities that may help you exploit the machine
- Final result
 - At the end of the lab, you should have a report “Notebook” with all discovered machine. For each machine you should have a list of running services with their vulnerabilities.
 - You can send us your Notebook report for feedback (it will not be graded).

Lab1 - Discovery

- Recommended steps
 - Get familiar with nmap for host discovery and port scanning (hint: google it or 'man nmap')
 - Find live hosts on the 10.10.40.0/24 range.
 - Perform port scan and service fingerprinting: determine service versions as precisely as possible.
 - Find relevant exploits on exploit-db (you can also search locally using 'searchsploit').
 - Validate your findings by performing a nessus scan
 - Get familiar with nessus vulnerability scanner (google for usage and ask us).

Discovery

- Final result example:

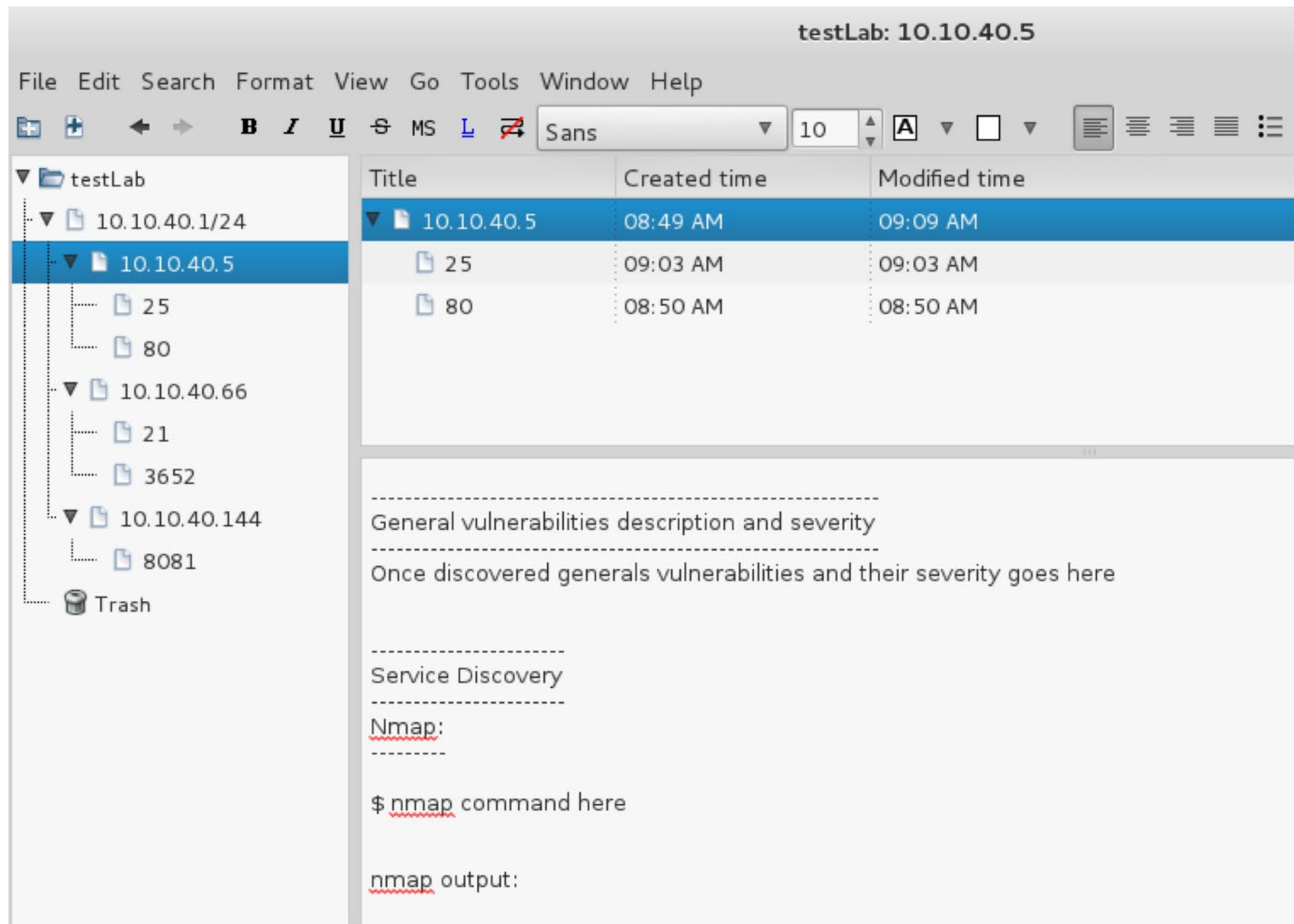
The screenshot shows a network discovery tool interface. On the left is a tree view of the discovered network structure. The main area on the right displays a table of discovered machines with columns for Title, Created time, and Modified time. The title bar indicates the current view is for 'testLab: 10.10.40.1/24'. The menu bar includes File, Edit, Search, Format, View, Go, Tools, Window, and Help. The toolbar contains various icons for file operations and formatting, including a font dropdown set to 'Sans' and a size dropdown set to '10'.

Title	Created time	Modified time
10.10.40.1/24	09:00 AM	09:05 AM
10.10.40.5	08:49 AM	09:05 AM
25	09:03 AM	09:03 AM
80	08:50 AM	08:50 AM
10.10.40.66	09:01 AM	09:02 AM
21	09:03 AM	09:03 AM
3652	09:03 AM	09:03 AM
10.10.40.144	09:02 AM	09:02 AM
8081	09:03 AM	09:03 AM

Host scan and discovered machines with generals information here

Discovery

- Final result example:



Discovery

- Final result example:

The screenshot shows a network discovery tool interface. On the left, a tree view displays the discovered network structure under 'testLab'. The tree includes a folder '10.10.40.1/24' which contains several sub-folders representing hosts: '10.10.40.5', '10.10.40.66', and '10.10.40.144'. Each host folder contains files representing discovered services, such as '25', '80', '21', '3652', and '8081'. A 'Trash' icon is also visible at the bottom of the tree.

On the right, a table displays the details for the selected host '10.10.40.5'. The table has three columns: 'Title', 'Created time', and 'Modified time'. The data rows are as follows:

Title	Created time	Modified time
10.10.40.5	08:49 AM	09:09 AM
25	09:03 AM	09:10 AM
80	08:50 AM	08:50 AM

Below the table, there is a section titled 'Service details' with a dashed border. It contains the text: 'here you can put all information about this service: name, version, vulns, etc...'. The word 'vulns' is underlined in red.

Lab2 - Exploit

- Vulnerabilities exploitation
- The goal of this lab
 - To get familiar with exploitation techniques and tools (metasploit, msfvenom, custom scripts,...)
 - Hands-on introduction to ethical hacking methods and CTF (Capture the Flag) methodologies
- Objective
 - Exploit the machines discovered during Lab1
 - Get the flag(s) !

Rules of Engagement

- Work in groups of 2 (or more)
 - 1 PC linked to infrastructure, 1 PC to google for info
- You have to use a VPN in order to connect to lab network (`\\eistore1\profs\ARS\cours\AST-2019\4.Lab`)
 - You receive your individual credentials by email
- Stick to the 10.10.40.0/24 range (no scanning of outside ranges).
- You shall not do a voluntary DoS on the infrastructure
 - Constantly check your ping and tcpdump
 - If you think that a system may be down due to your activities, tell us and we will perform a reset of the machine and corresponding services.
- If you succeeded in obtaining the flag you can validate it with us (send us an email with vulnerability explanation and flag).
 - This assignment is not graded.

Useful software

- A list of useful penetration testing tools.
 - Nmap
 - Dradis
 - Burp suite
 - Metasploit
 - Msfvenom
 - Nessus
 - Wireshark
 - Exploit-db (website)

Not all needed for this lab !