AST

Audit de Sécurité Technique

Practical Lab

Discovery & Exploitation

Abraham Rubinstein & Jean-Marc Bost

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

heig-vd
HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.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

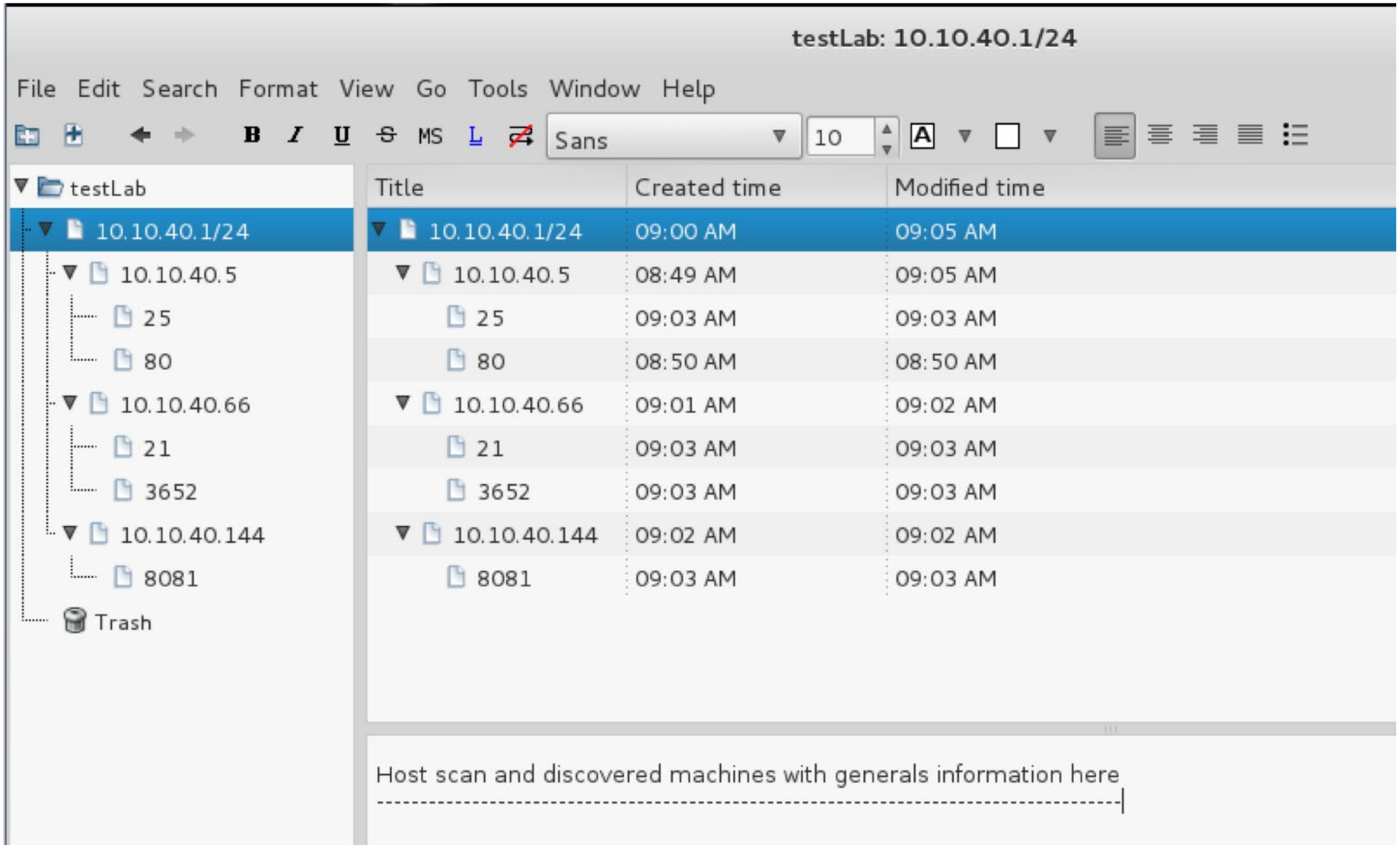
- The goal of this lab
  - Get familiar with network recon techniques (nmap, vulnerability scanning, services discovering, exploit-db search)
  - Hands-on introduction to ethical hacking methods and CTF (Capture the Flag) methodologies
  - Get familiar with a reporting tool to keep trace of your findings
- 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).

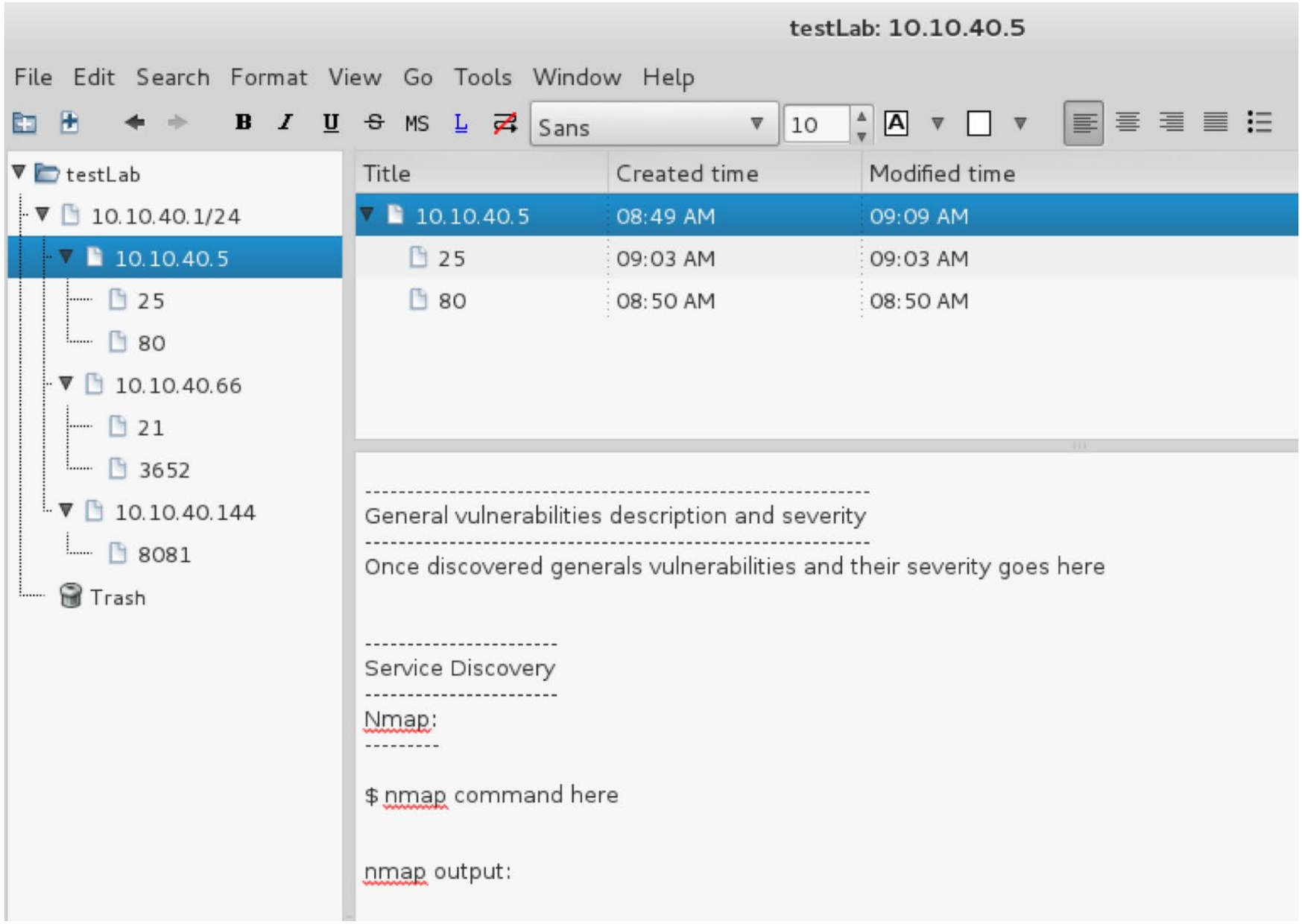
Discovery

- Final result example:



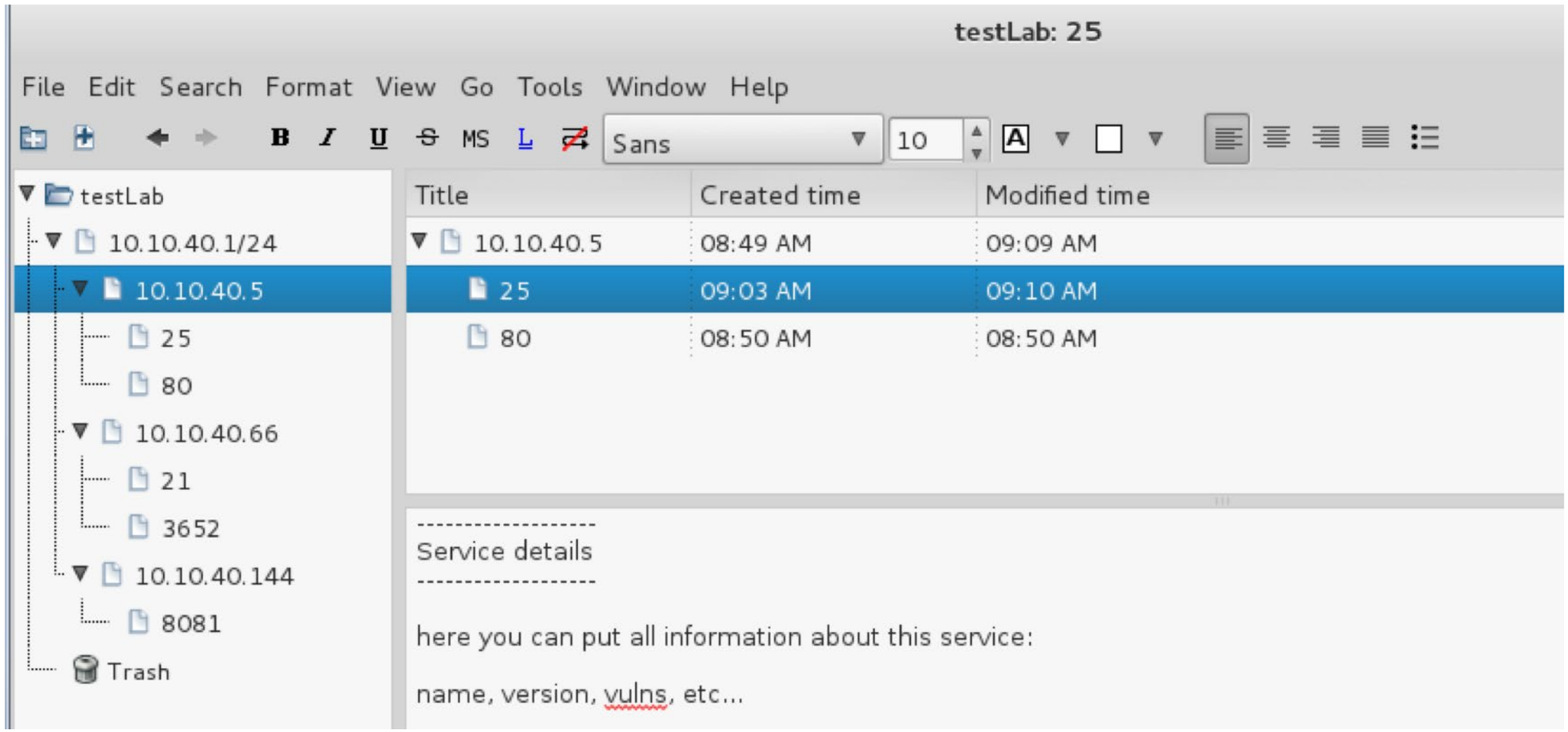
Discovery

- Final result example:



Discovery

- Final result example:



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 assignement 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 !