AST

Audit de Sécurité Technique

Chapter 2.4
Toolbox

Jean-Marc Bost

jean-marc.bost@heig-vd.ch

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

Set of tools for technical security assessments

- What do you use?
  - Windows
  - Linux
  - OS X

- Recommendation is to have all three of them, or at least Windows and Linux
  - Don’t think of them as different operating systems
  - Thinks of them as set of tools
- Setup a virtualized environment on you machine (VMWare)
  - Deploy images of Windows and Linux boxes so that you can easily switch between
- Today’s average Portable PC (quad-core)
  - Can easily run several OS in parallel
  - Images allow easily to backup, roll-back and deploy a fresh/clean version of the OS

Testing platform

- The Kali linux distribution which superseded historical BackTrack (BT) linux is seen as a de-facto standard platform to help you with your pentest tasks
  - Debian-based distribution
  - More than 300 tools for pentest and data forensics
  - Active online support community
  - Easy to install and start using

If you are an Arch Linux fan, you might want to give BlackArch a try

Kali

- Download from www.kali.org
  - Either an ISO from http://www.kali.org/downloads/
  - VMWare image from http://www.offensive-security.com/kali-linux-vmware-arm-image-download/
    - Download, unzip (`7z x Kali-Linux-2019.3-vm-amd64.7z`) and open the image in VMPlayer
    - default username and password: root/toor
    - remember to change the root password
    - `apt-get update && apt-get upgrade`
  - In normal circumstances if running a WMPlayer, ensure that you are using **Bridged network** option for your virtual network adapter
    - If you are on HEIG-VD WLAN — use NAT !

Non-root user

- When installed, Kali linux uses root user for all tasks
- It is a good security practice to add an additional user with non-root privileges
  - `useradd -m noroot`
    `passwd noroot`
    `usermod -a -G sudo noroot`
    `chsh -s /bin/bash noroot`
  - Replace the `noroot` by whatever you prefer

Install MultiArchitecture support

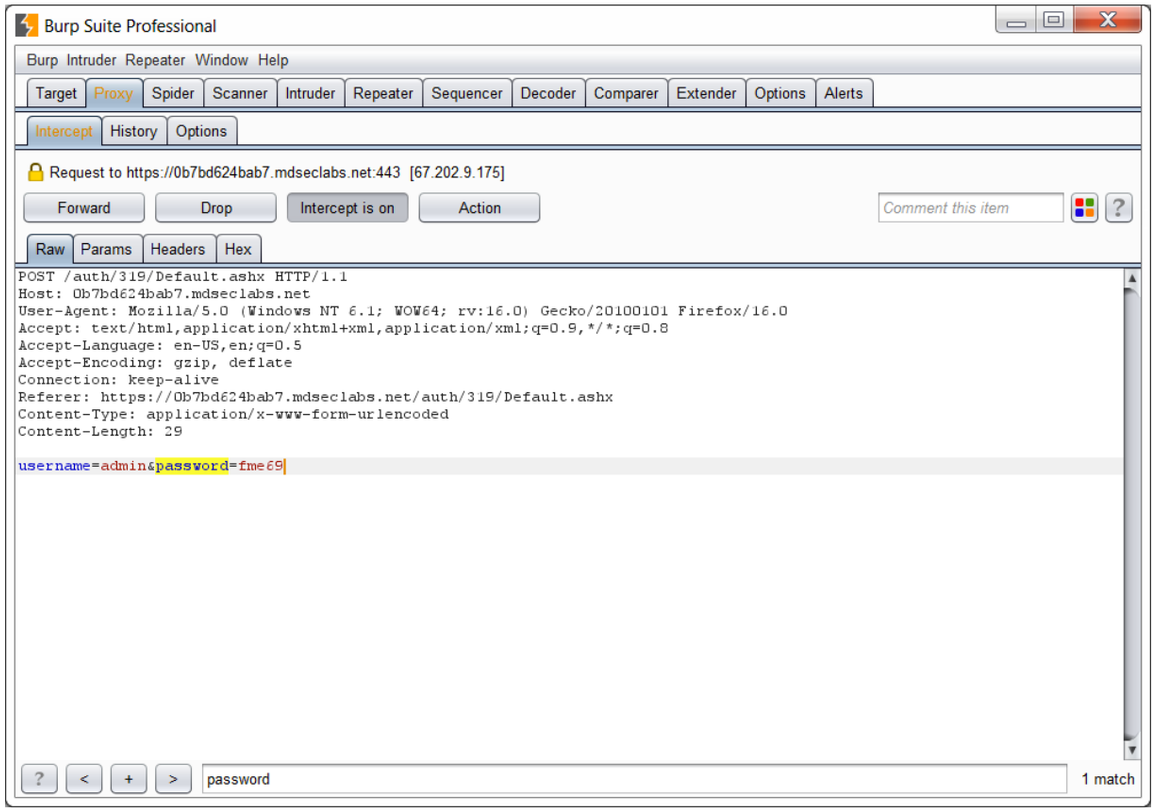
- By default Kali comes with 64 bit architecture
  - ```
    sudo dpkg --add-architecture i386
    sudo apt-get update
    sudo apt-get upgrade
    ```
  - Enables 32-bit support
  - Useful for applications supporting only 32-bit
    ```

Default repositories

- The default package repositories that should be present in `/etc/apt/sources.list` are listed as follows; if not present, edit the `sources.list` file to include them
  - `deb http://http.kali.org/kali kali-rolling main non-free contrib`

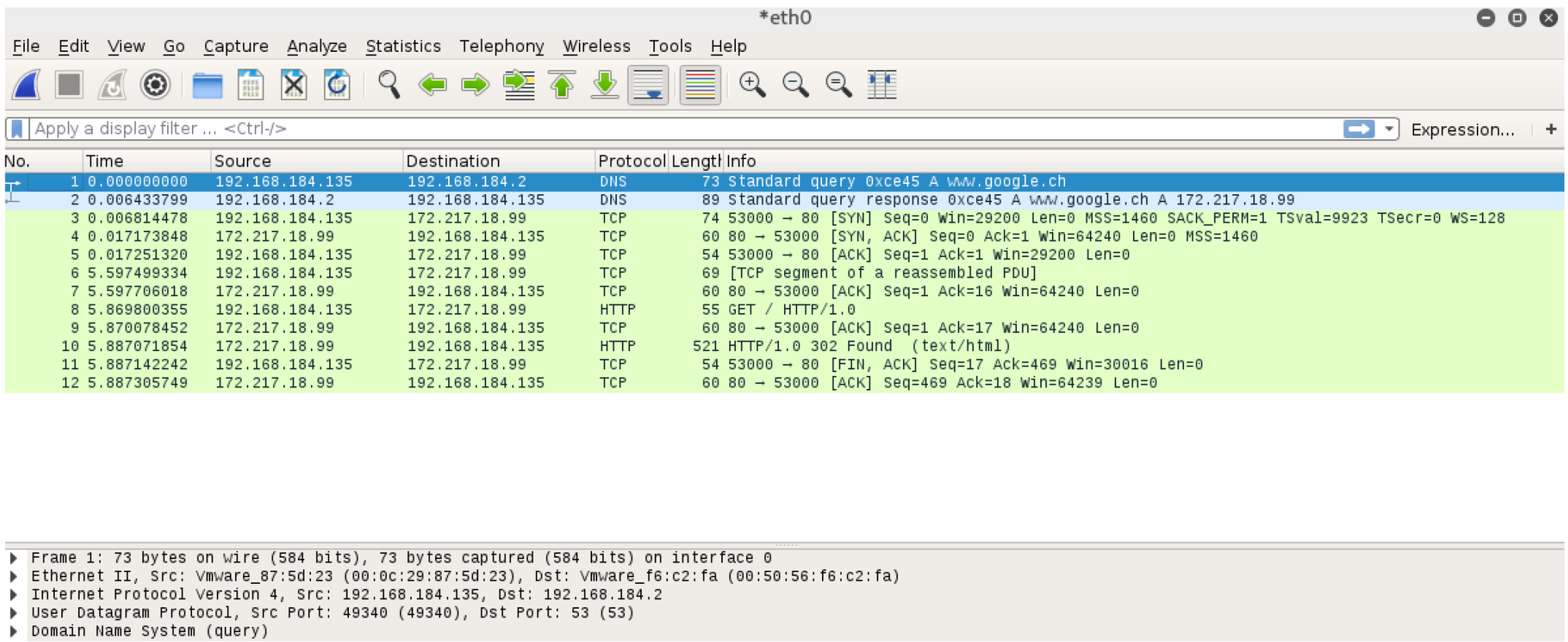
Burp Suite

- The most well-known toolbox for web hacking
- Comprises:
  - Proxy - intercept and modify requests
  - Spider - discover content
  - Scanner - vulnerabilities scanner
  - Intruder/repeater - attack tools
  - …
- Free version available in Kali



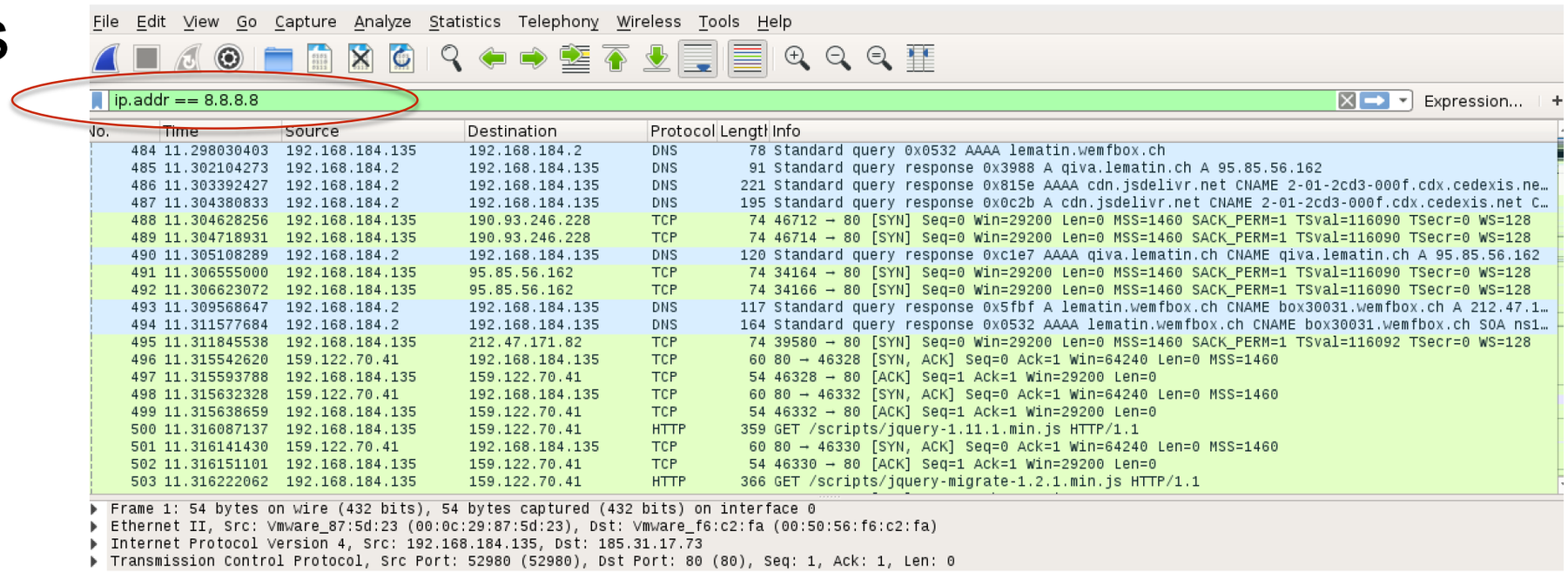
Wireshark

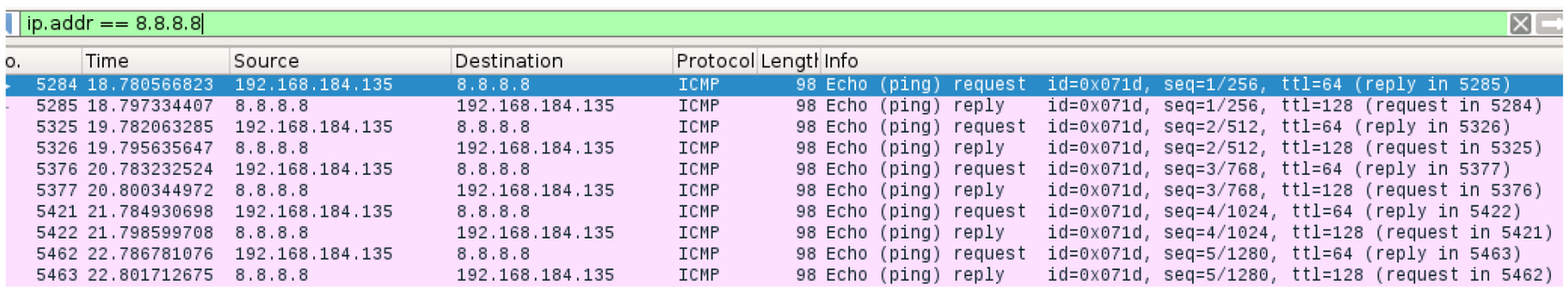
- The ultimate packet sniffer
  - Understanding/reverse engineering of protocols
  - Network debugging
  - Traffic analysis



Wireshark

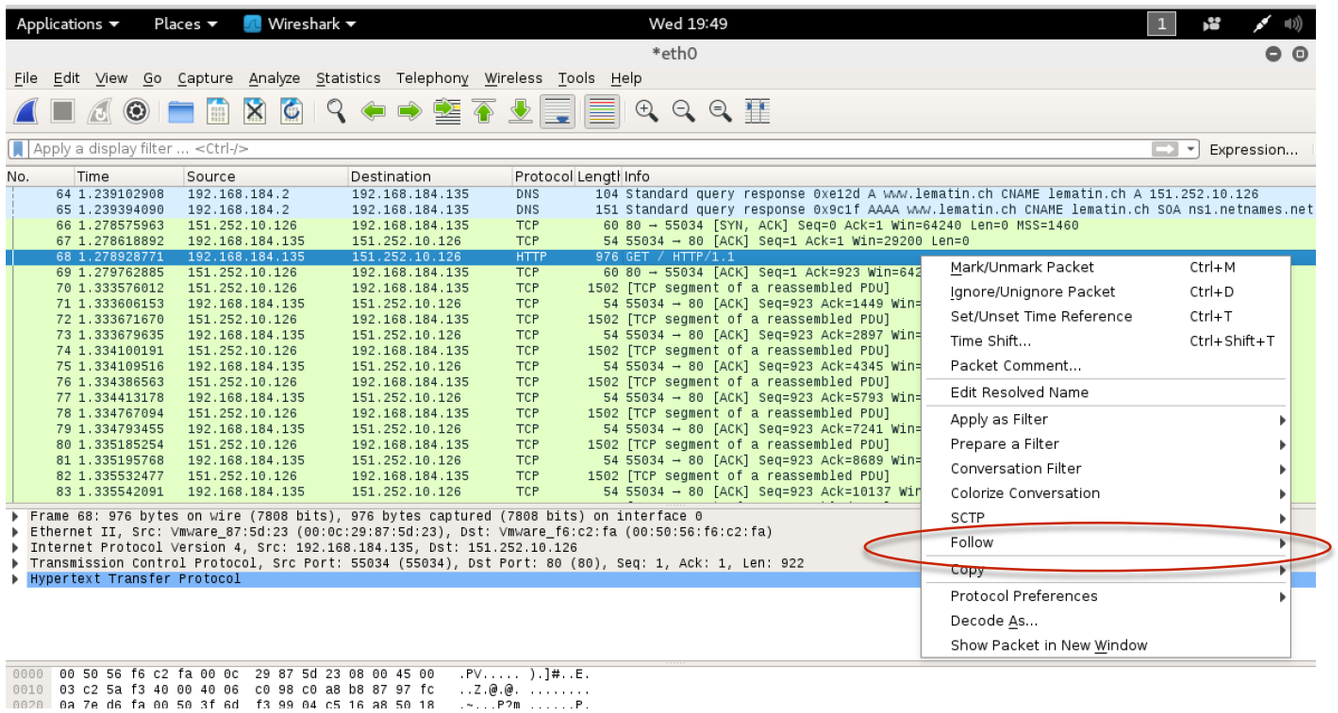
- Capture filters
- Display filters





Wireshark

- Reconstructing streams



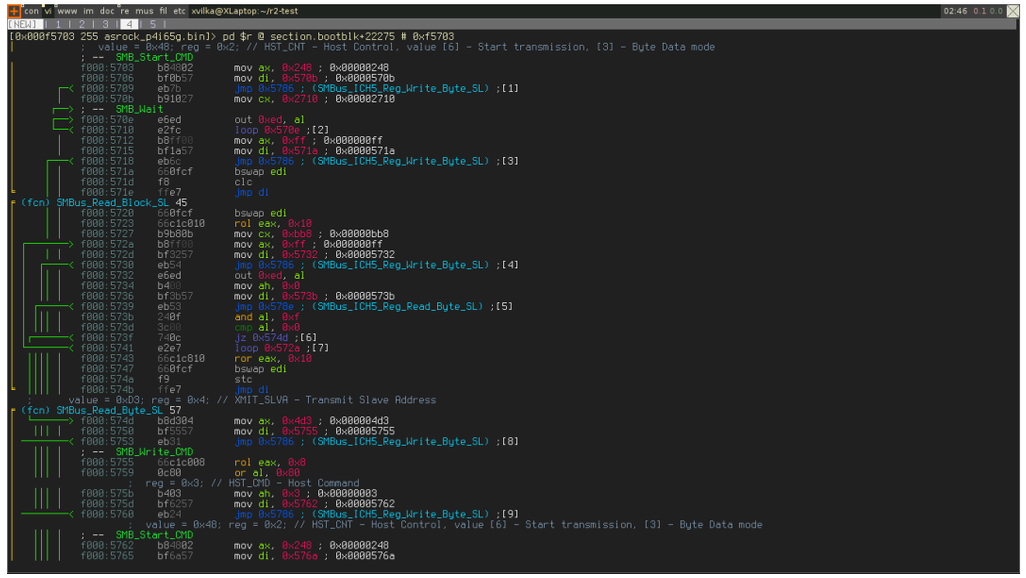
Last but not least

- Netcat
  - Hacker's Swiss Army Knife
  - Read and write tcp ports
  - Transferring files, remote administration, reverse shells,…
- Tcpdump
  - Command-line packet capture and analyser
  - When GUI is not available
  - Fast
  - To capture for further analysis with Wireshark:

```
$ tcpdump -i <interface> -s 65535 -w <some-file>
```

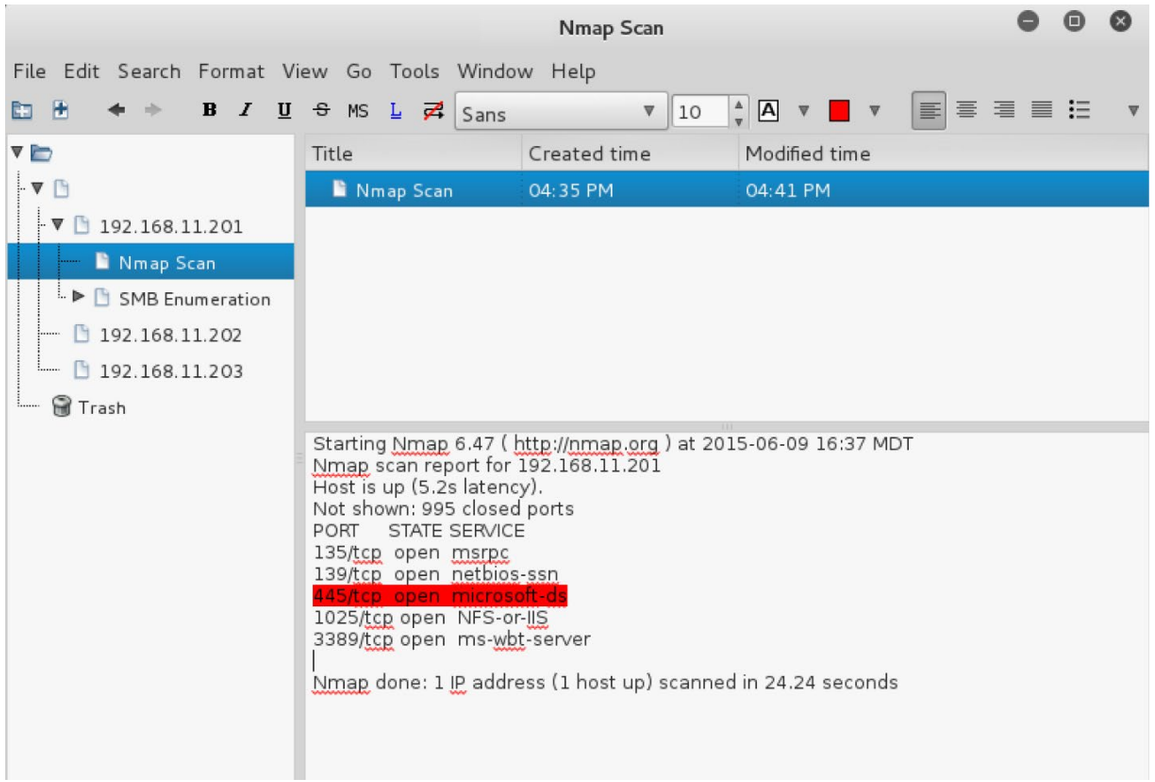
Binary reverse engineering

- IDA Pro - Fully Featured Disassembler
  - The weapon of choice when it comes to reverse engineer (any) binary
  - Quite expensive
  - Demo/free old version officially available from
    `https://www.hex-rays.com/products/ida/support/download_freeware.shtml`
- Ghidra
  - https://ghidra-sre.org
  - Developed by the NSA (Java/Swing)
  - Free, open source
- Radare2 is a free alternative
  - https://www.radare.org
  - Included in Kali



Keeping notes through your work

- KeepNote available in Kali linux
- To organize the information gathered during your security project
- Can do screen grabbing and export to HTML



- You are of course free to use any application of your choice as long as you track and write down your findings.

Searching for exploits

- There are several source for public exploits
- A good and reliable source: Exploit-db (www.exploit-db.com)
  - Available in your kali distro with `searchploit` command