

Introduction and Preparation



SoftUni Team
Technical Trainers



SoftUni



Software University

<https://softuni.bg>

Have a Questions?

sli.do

#Cyber_Security

1. Introduction to Reconnaissance

2. Environment Set-up

- Configuring Kali-Linux for Information Gathering
- Installing Tools





Course Requirement

- **Kali Linux** (<https://www.kali.org/>) – Recommended
- **ParrotOS** (<https://www.parrotsec.org/>)
- **Black Arch Linux** (<https://blackarch.org/>)
- **CommandoVM** (<https://github.com/mandiant/commando-vm>)





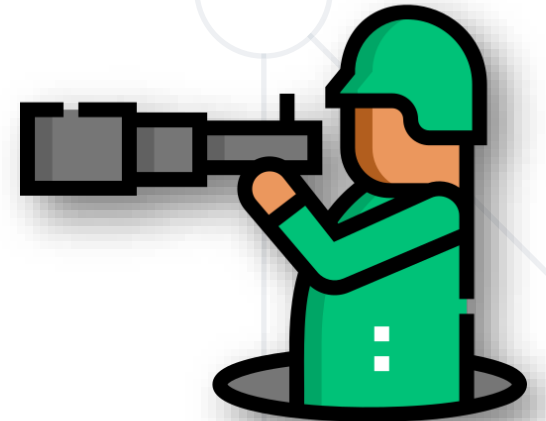
Introduction to Reconnaissance

- **Reconnaissance** is utilizing creativity + technical knowledge to obtain sensitive, personal or publicly available information about targeted asset
- **Reconnaissance** is the first step of the real engagements and operations
 - You can't exploit something without knowing what it is, logical right?
- **Reconnaissance** is the most important part of the security assessments known as penetration testing / red teaming operations
 - Deep understanding of the target leads to finding / exploiting vulnerabilities



Types of Reconnaissance

- **Passive reconnaissance** is the process of obtaining information about the target, by utilizing OSINT (Open Source INTelligence)
- OSINT is a set of techniques and tools for obtaining information about a target, in a completely stealthy way



- For example, the following example activities are considered OSINT:
 - Stalking Social Networks (We are performing requests towards their servers)
 - Searching for Code Repositories / Pastebins (Same)
 - Utilizing third party scanning tools (like DNSdumbster)
 - Querying Google and other search engines.
 - Many, many more...
- **PASSIVE RECONNAISSANCE DOES NOT GENERATE TRAFFIC TO THE TARGET SIDE!**

- **Active reconnaissance** is the process of obtaining information about the target, by utilizing aggressive tools like scanners, fuzzers and more.
- Example Active Reconnaissance Activities:
 - Port scan (nmap, masscan)
 - Vulnerability scanning (nessus, burpsuite)
 - Directory brute-forcing (gobuster, dirb)
 - Parameter fuzzing (wfuzz, ffuf)
 - Front-end source code review
 - Many, many more
- **ACTIVE RECONNAISSANCE DOES GENERATE TRAFFIC TO THE TARGET SIDE!**



Environment Set-up

- `sudo apt-get update`
- `sudo apt-get upgrade`
- "**sudo**" is important, the commands will not work without it
- "**sudo**" grants allows you to execute commands with "**root**" privileges
- "**root**" privileges are the highest privileges in a UNIX-like system, meaning the "root" user can do pretty much anything (example: deleting the boot loader)
- Installing updates requires root privileges

Choose Your Note Taking Software

- The reconnaissance process can be long, and the amount of generated output can be massive
- That's why we need to store the output in a useful and "**easy to work with**" way
- Best note-taking choices are:
 - Obsidian (<https://obsidian.md/download>)
 - CherryTree (<https://www.giuspen.net/cherrytree/>)
 - One Note (<https://www.microsoft.com/en-us/microsoft-365/onenote/digital-note-taking-app>)

■ Pros / Cons:

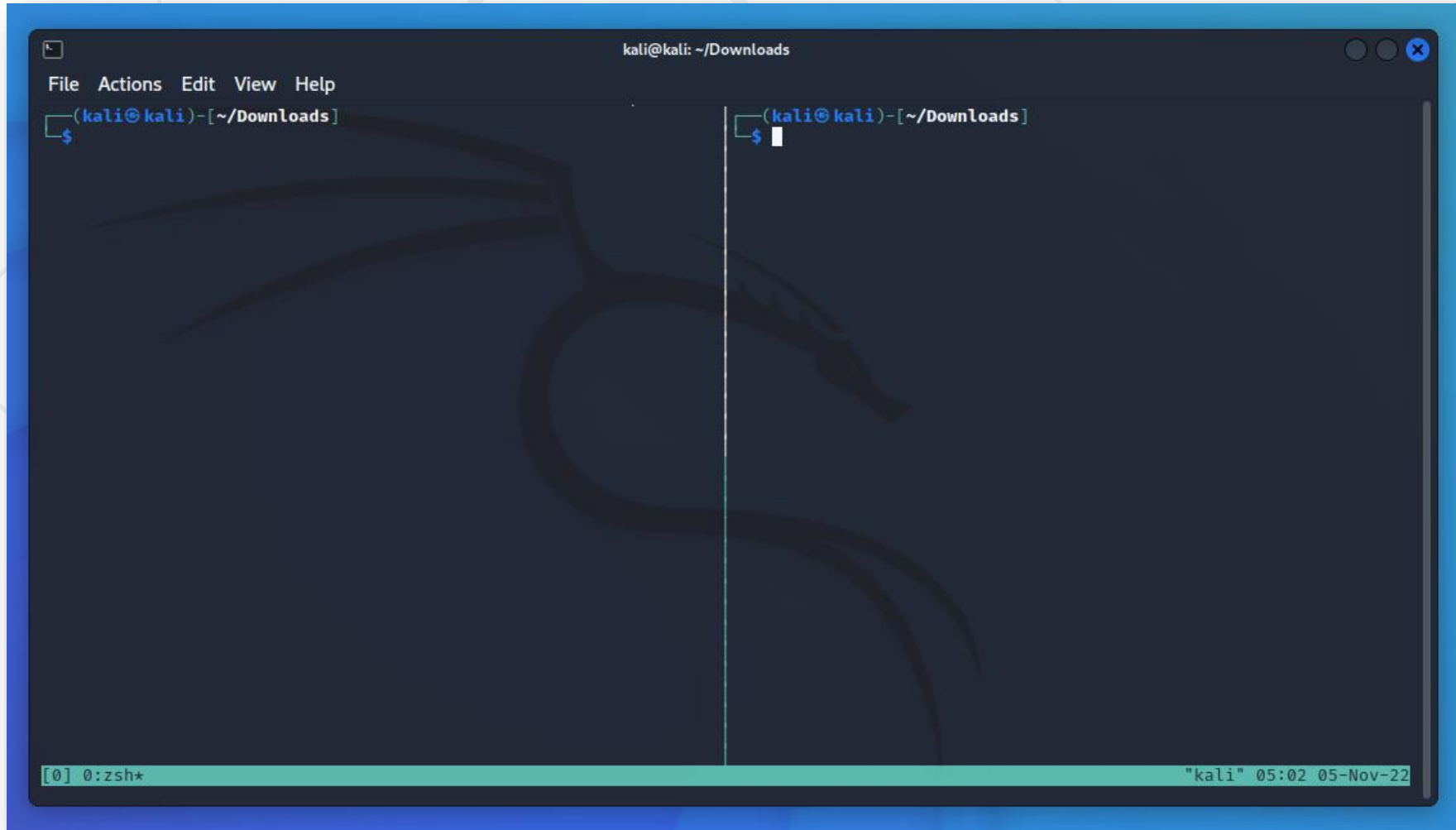
- Obsidian and CherryTree are local, meaning no cloud would access your data (**Pros**)
- CherryTree is using it's own file format, making it hard to migrate data (**Cons**)
- Obsidian uses .md format, making it extremely easy to copy / migrate data (**Pros**)
- Beside being cloud application, One Note does not have any other cons (**Pros**)

- In the course scope, we will be using Obsidian, since it is local based, highly customizable and easy to use
 - Download Obsidian (<https://obsidian.md/download>) (64 bit installer (Windows) / appimage (Linux))
 - Installing Obsidian on Windows, simply start the installer and follow the steps
 - Installing the Obsidian on Linux is not needed since it is preinstalled, you need just to start it with `./Obsidian-1.0.3.AppImage`

- During engagements, we must organize our environment. One of the ways of doing that is by using console software, allowing us to perform multi-tab operations
- Best console management software choices are:
 - Tmux (<https://github.com/tmux/tmux/wiki>)
 - Terminator (<https://github.com/gnome-terminator/terminator>)
 - Konsole (<https://konsole.kde.org>)
- Pros / Cons:
 - Tmux is hard to use (Cons)
 - Terminator and Konsole are beginner friendly (Pros)

Installing Tmux

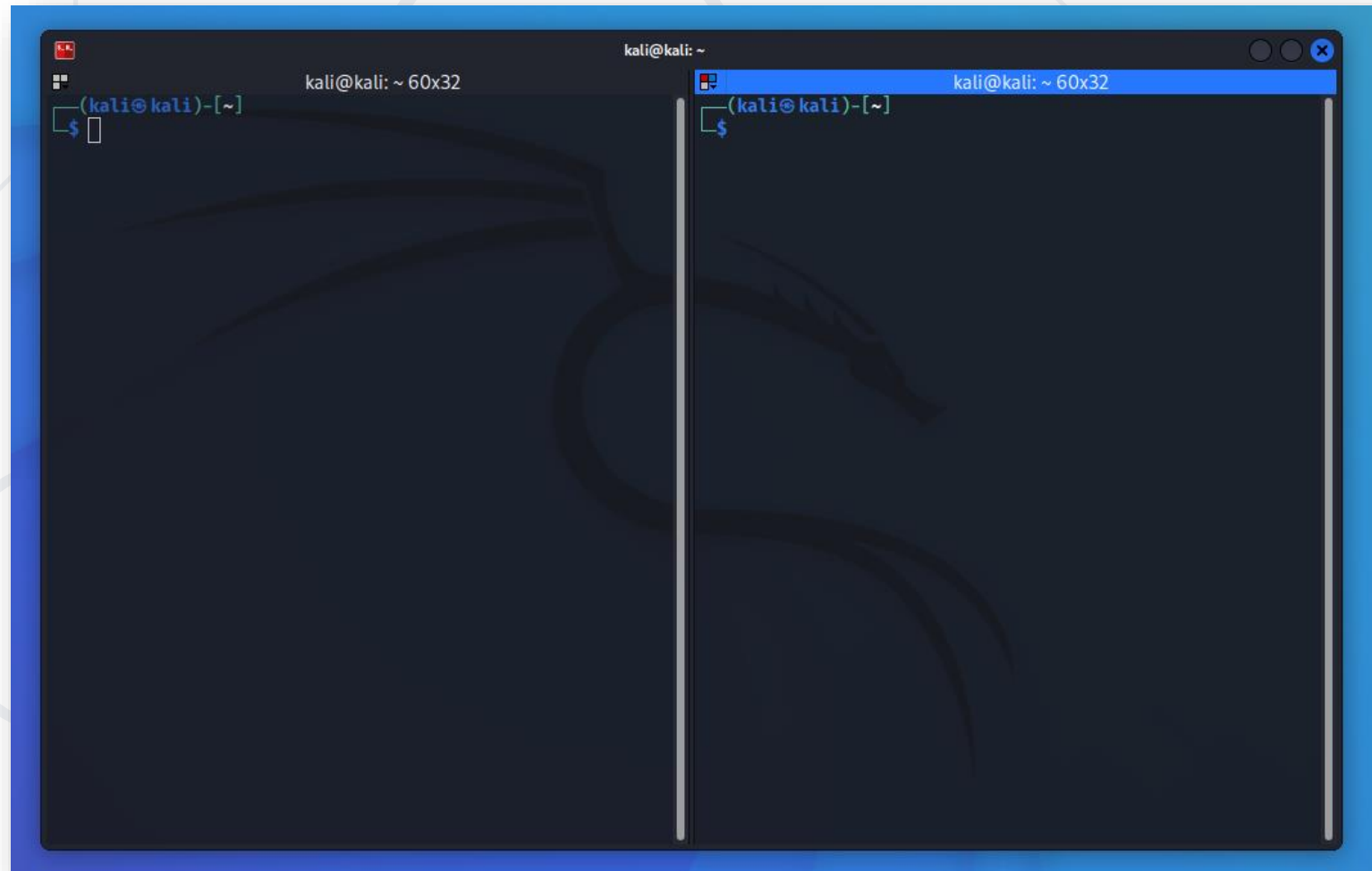
- `sudo apt-get install tmux`



The screenshot shows a terminal window titled "kali@kali: ~/Downloads". The window has a menu bar with "File", "Actions", "Edit", "View", and "Help". The prompt is "(kali@kali)-[~/Downloads]" followed by a dollar sign "\$". The terminal is split into two panes by a vertical line. The left pane shows the prompt and a green status bar at the bottom with "[0] 0:zsh*". The right pane shows the prompt and a green status bar at the bottom with "\"kali\" 05:02 05-Nov-22".

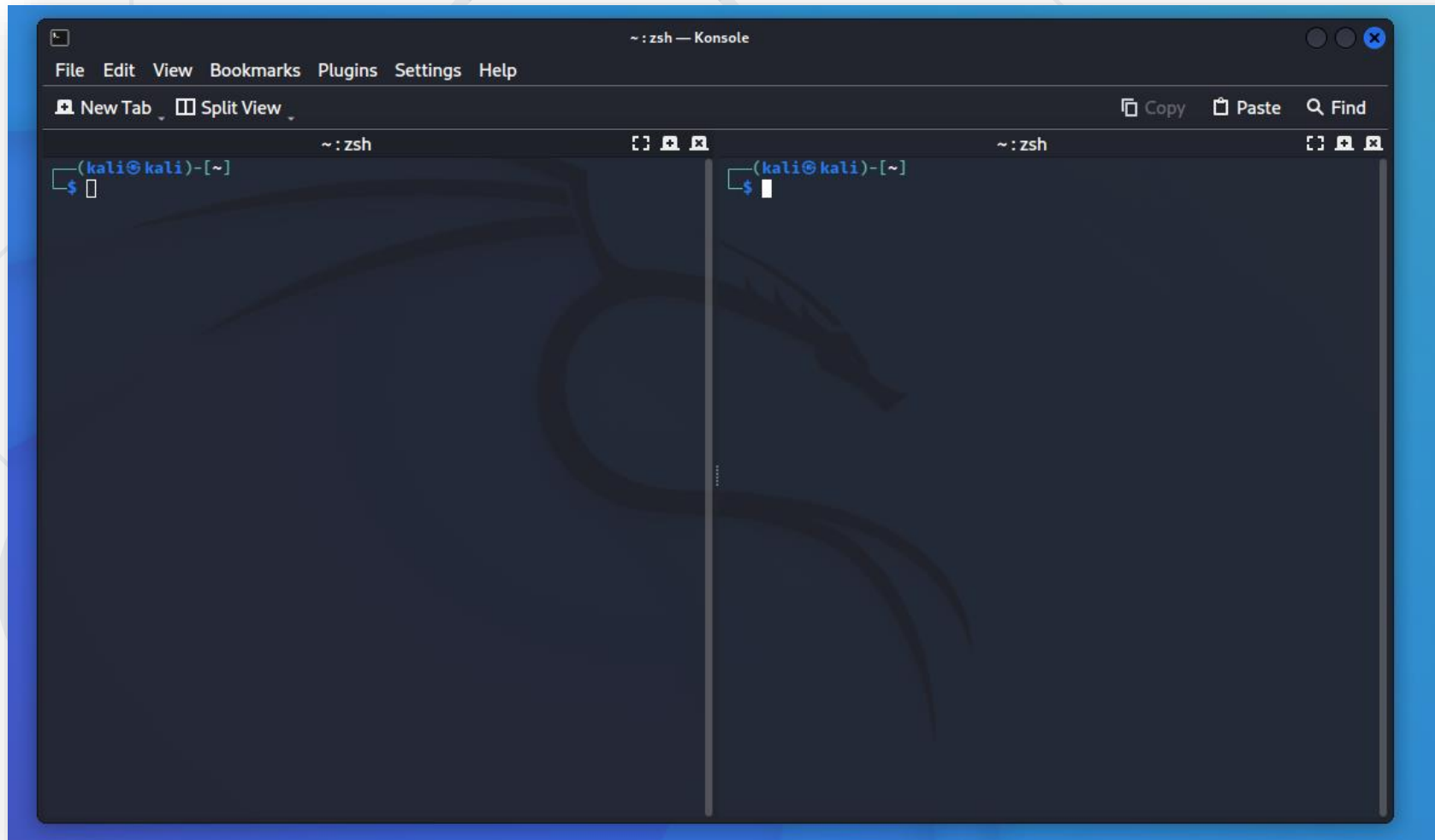
Installing Terminator

- `sudo apt-get install terminator`



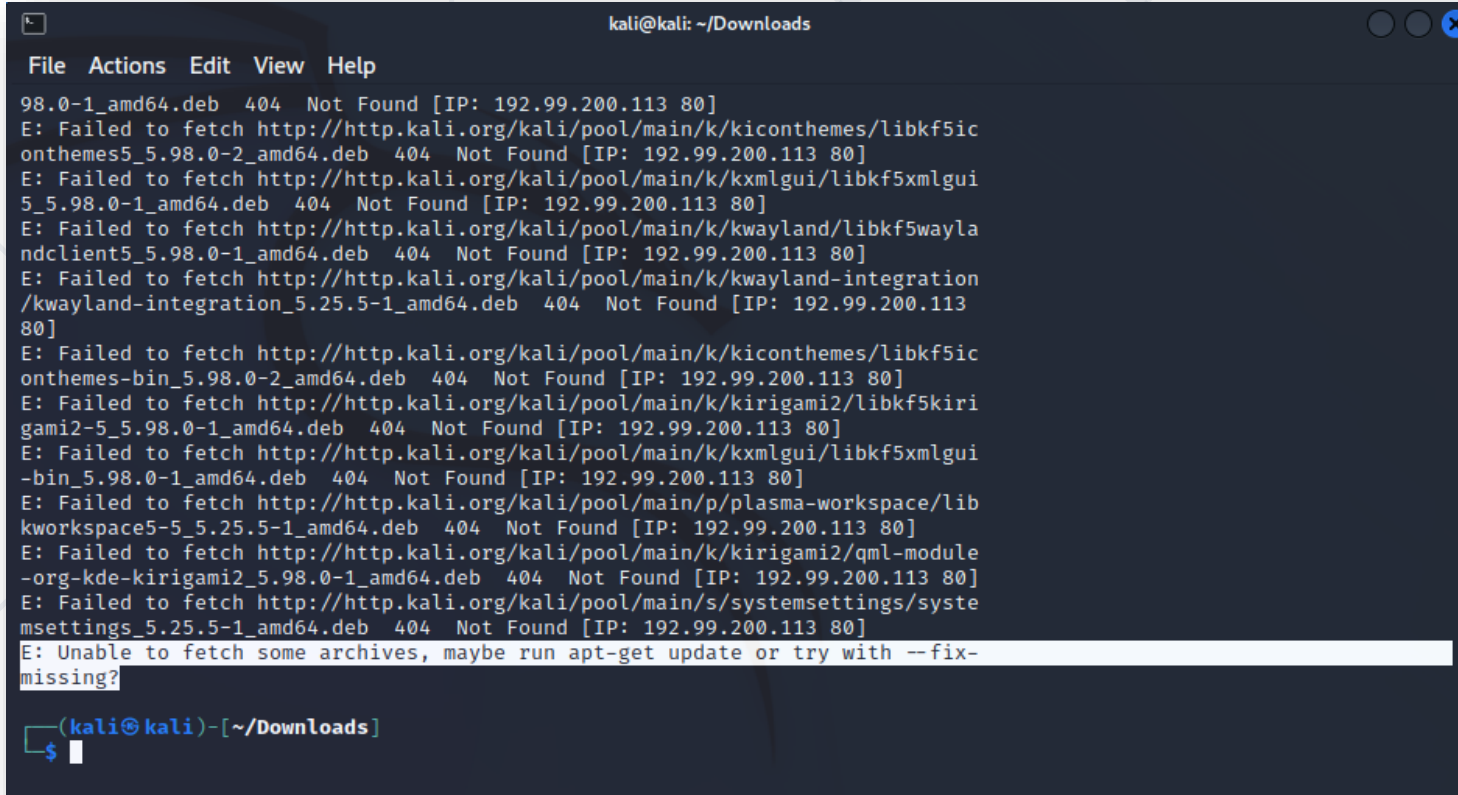
Installing Konsole

- `sudo apt-get install terminator`



In Case of Error

- Like this:

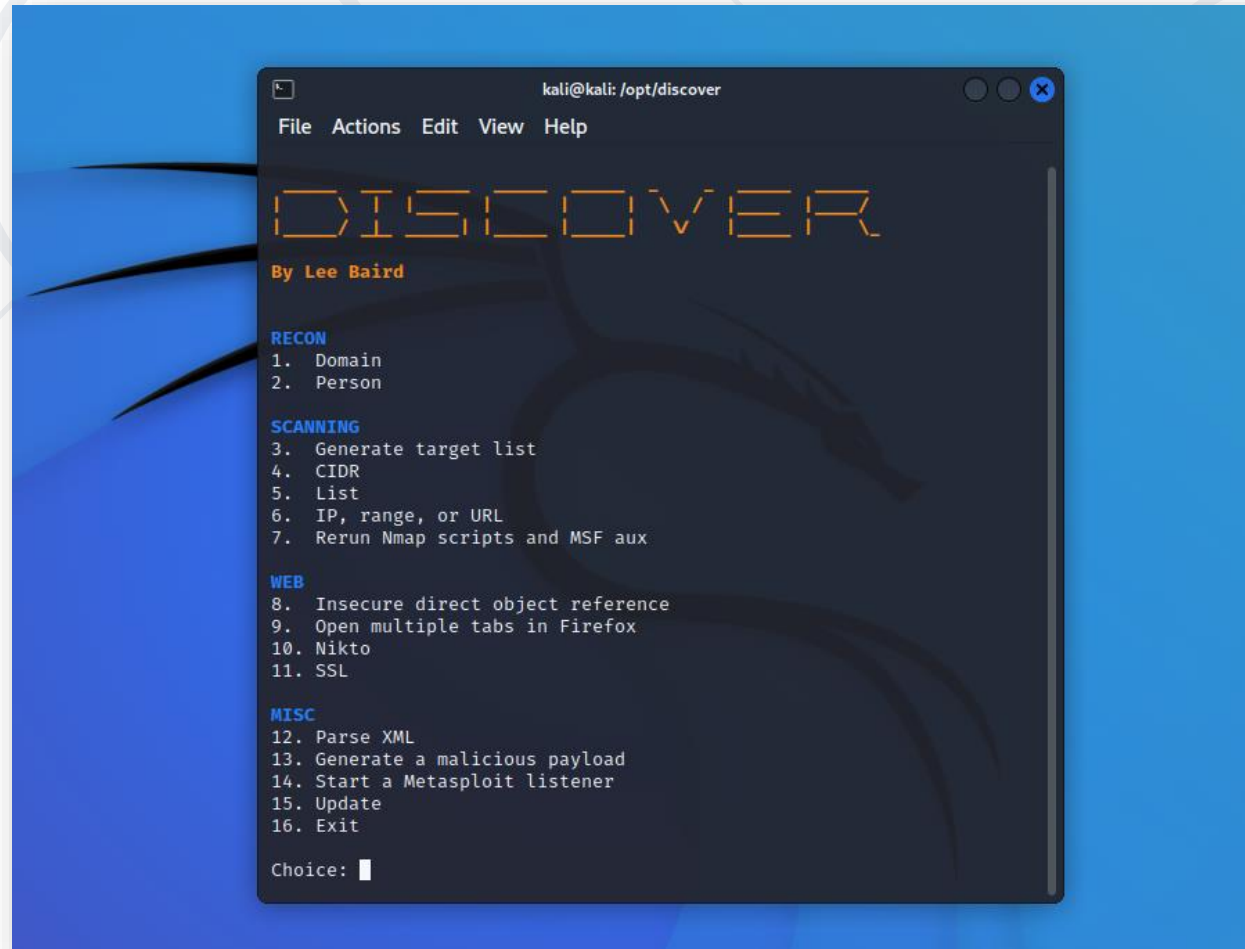


```
kali@kali: ~/Downloads
File Actions Edit View Help
98.0-1_amd64.deb 404 Not Found [IP: 192.99.200.113 80]
E: Failed to fetch http://http.kali.org/kali/pool/main/k/kiconthemes/libkf5ic
onthemes5_5.98.0-2_amd64.deb 404 Not Found [IP: 192.99.200.113 80]
E: Failed to fetch http://http.kali.org/kali/pool/main/k/kxmlgui/libkf5xmlgui
5_5.98.0-1_amd64.deb 404 Not Found [IP: 192.99.200.113 80]
E: Failed to fetch http://http.kali.org/kali/pool/main/k/kwayland/libkf5wayla
ndclient5_5.98.0-1_amd64.deb 404 Not Found [IP: 192.99.200.113 80]
E: Failed to fetch http://http.kali.org/kali/pool/main/k/kwayland-integration
/kwayland-integration_5.25.5-1_amd64.deb 404 Not Found [IP: 192.99.200.113
80]
E: Failed to fetch http://http.kali.org/kali/pool/main/k/kiconthemes/libkf5ic
onthemes-bin_5.98.0-2_amd64.deb 404 Not Found [IP: 192.99.200.113 80]
E: Failed to fetch http://http.kali.org/kali/pool/main/k/kirigami2/libkf5kiri
gami2-5_5.98.0-1_amd64.deb 404 Not Found [IP: 192.99.200.113 80]
E: Failed to fetch http://http.kali.org/kali/pool/main/k/kxmlgui/libkf5xmlgui
-bin_5.98.0-1_amd64.deb 404 Not Found [IP: 192.99.200.113 80]
E: Failed to fetch http://http.kali.org/kali/pool/main/p/plasma-workspace/lib
kworkspace5-5_5.25.5-1_amd64.deb 404 Not Found [IP: 192.99.200.113 80]
E: Failed to fetch http://http.kali.org/kali/pool/main/k/kirigami2/qml-module
-org-kde-kirigami2_5.98.0-1_amd64.deb 404 Not Found [IP: 192.99.200.113 80]
E: Failed to fetch http://http.kali.org/kali/pool/main/s/systemsettings/syste
msettings_5.25.5-1_amd64.deb 404 Not Found [IP: 192.99.200.113 80]
E: Unable to fetch some archives, maybe run apt-get update or try with --fix-
missing?
(kali@kali)-[~/Downloads]
$
```

- `sudo apt-get update --fix-missing`

Installing and Running Discover

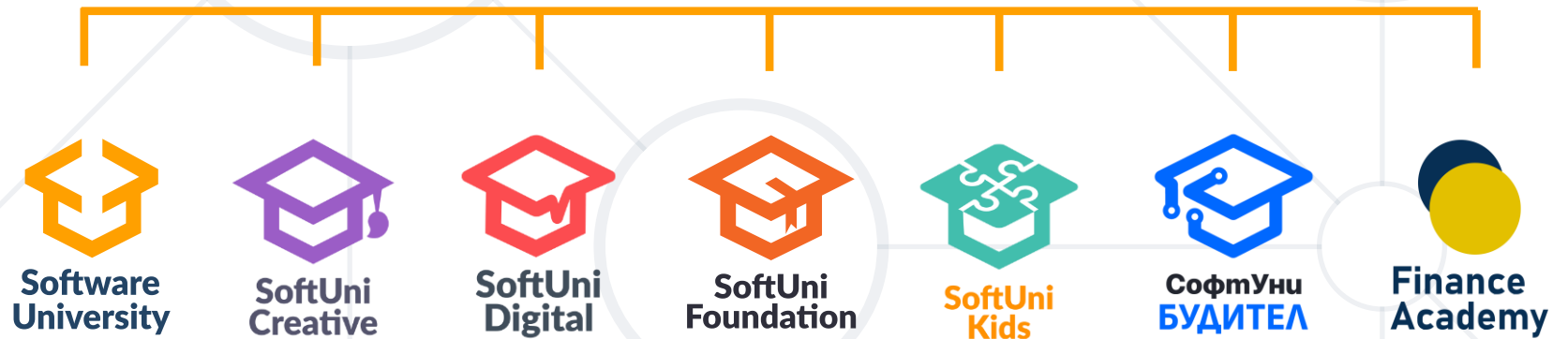
1. `sudo git clone https://github.com/leeбайд/discover`
2. `cd /opt/discover/`
3. `sudo ./discover.sh`



- Course Requirement
- Introduction to Reconnaissance
 - Information Gathering in a Nutshell
- Types of Reconnaissance
 - Passive
 - Active
- Environment Set-up



Questions?



SoftUni Diamond Partners



THE CROWN IS YOURS



- Software University – High-Quality Education, Profession and Job for Software Developers
 - softuni.bg, about.softuni.bg
- Software University Foundation
 - softuni.foundation
- Software University @ Facebook
 - facebook.com/SoftwareUniversity



- This course (slides, examples, demos, exercises, homework, documents, videos and other assets) is **copyrighted content**
- Unauthorized copy, reproduction or use is illegal
- © SoftUni – <https://about.softuni.bg/>
- © Software University – <https://softuni.bg>

