RESEARCH AND BUILD TOOLS TO SUPPORT THE NETWORK SYSTEM PENETRATION TESTING PROCESS

GSP24IA07

PROJECT INFORMATION

Supervisor : MR. Hồ Hải

Members :

Nguyen Dinh Quan - SE151007
Tran Minh Nhat - SE150956
Nguyen Minh Tam - SE151041
Nguyen Thanh Nhan - SE151405

Content OutLine

1.Project penetration testing

- 1.1 Policy
- 1.2 Network Model

2.CheckList

3.Demo

- 3.1 Scenario 1
- 3.2 Scenario 2

4. Conclusion

Policy

Learning and Knowledge Update

Security Testing

Reporting and Evaluation

Ethics and Responsibility

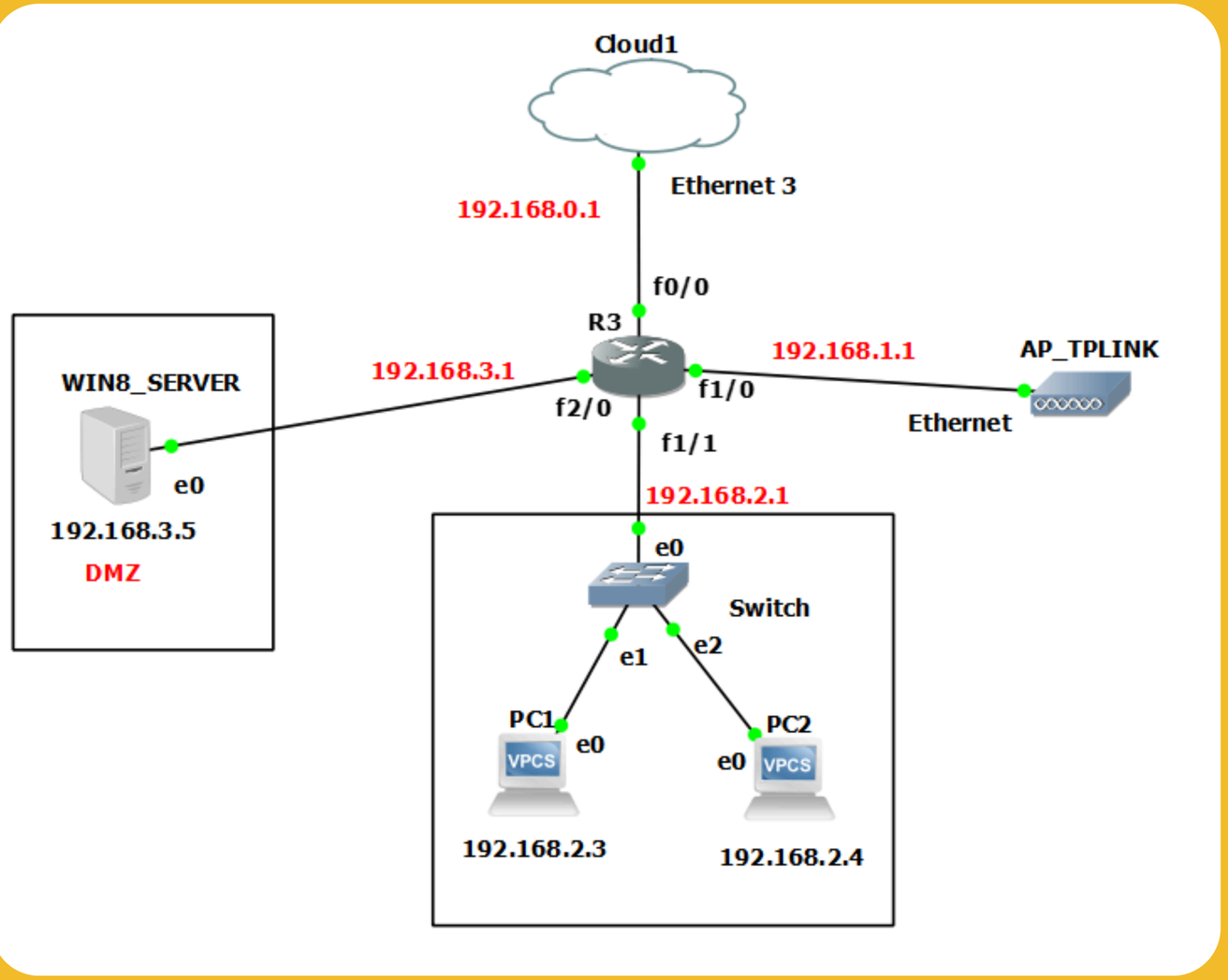
Pentest demo policy

Agreement and Legal Compliance

Recording and Information Security

Scope Definition

1.2 Network Model



Virtual device

- Router
- Switch

VMware

- Windows 8.1(Winserver)
- PC1 PC2 are vpcs are internal machines

Real equipment

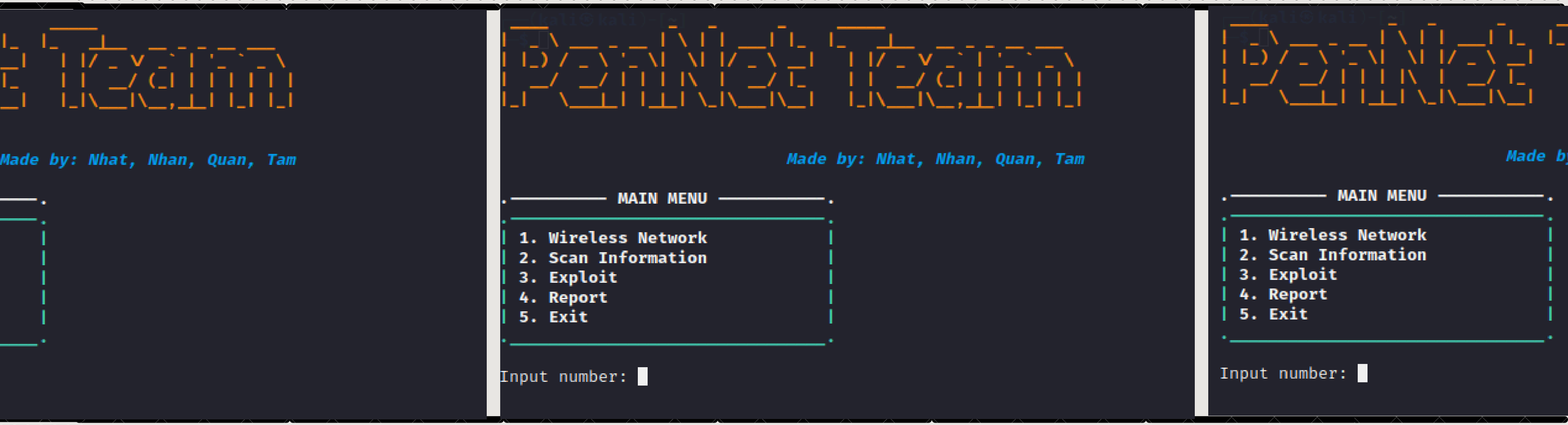
- AccessPoint

2.CheckList

- Port Scanning
- List open ports
- List suspicious ports that may be stealth
- Password Service Strength Testing
- Examine the use of standard and nonstandard protocols
- Examine the patches applied to the system
- Create Network Modem

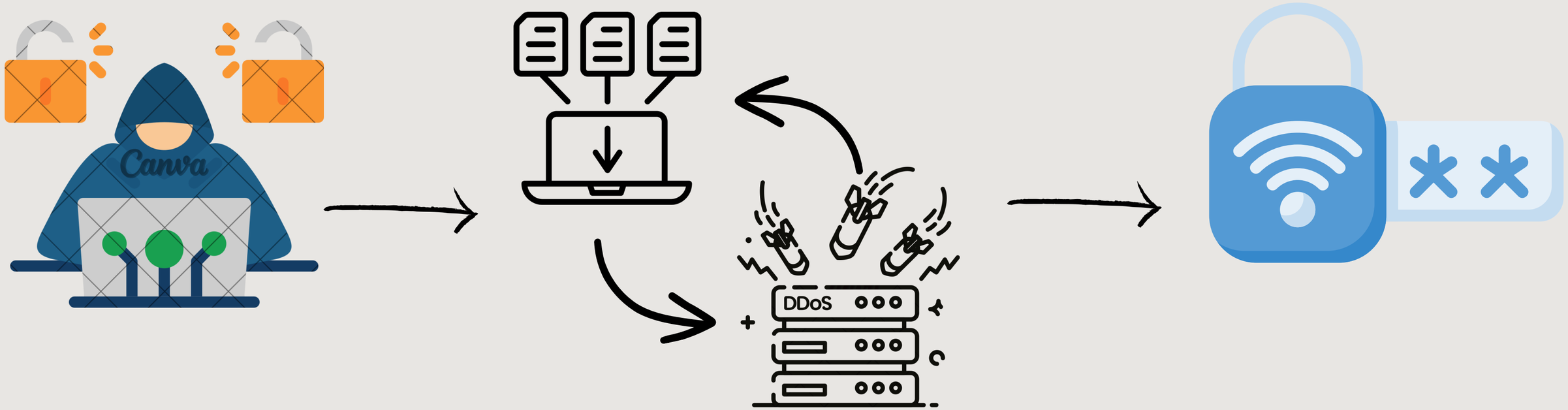
- Check for BruteFroce
- Check for backdock
- Check for default Credential
- Check for weak encryption
- Check Router
- Check Access Point
- Check for DOS
- Test for port (23)
- Check for FTP vulnerabilities

3.Demo


Made by: Nhat, Nhan, Quan, Tam
MAIN MENU
1. Wireless Network
2. Scan Information
3. Exploit
4. Report
5. Exit
Input number:
Made by: Nhat, Nhan, Quan, Tam
MAIN MENU
1. Wireless Network
2. Scan Information
3. Exploit
4. Report
5. Exit
Input number:

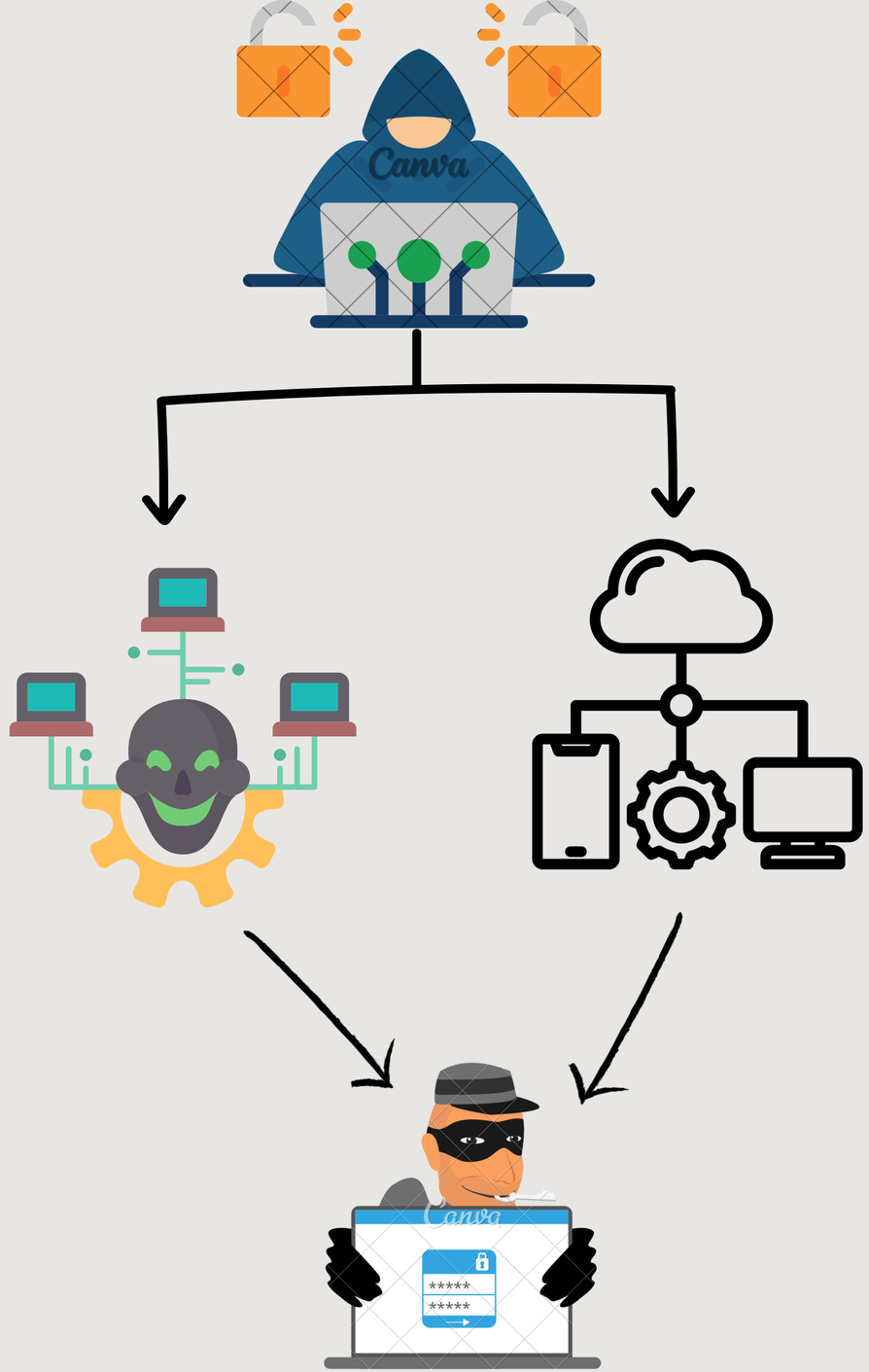
3.1 Sceniro 1

In the first scenario, we will use GNS3 to operate a virtual network model using virtualized routers to perform IP allocation for Access Points and the implementation environment is based on no firewall. This method is often implemented and tested to attack and test the safety and security of network devices. Specifically about passwords and traffic.



3.2 Sceniro 2

After Scenario 1, we already have the access point's wifi password because of the laxity in setting security policies for network devices, so we can scan the devices that are connected to the network infrastructure. From there, we can identify important locations such as routers or dmz servers and internal devices. Because this is a plan to follow a process that has been simulated, we have a diagram of the The network device then recognizes the router and performs testing to obtain the username and password in the device's web config to change the device's settings.



4.Report

PN Report

1. Scan Multiple Subnets: 192.168.1.0/24

- Active hosts: 192.168.1.1

2. Scan Services: 3

- Active ports:

    21/tcp - state:filtered - service:ftp

    22/tcp - state:filtered - service:ssh

    23/tcp - state:open - service:telnet Cisco IOS telnetd

    25/tcp - state:filtered - service:smtp

    80/tcp - state:open - service:http Cisco IOS http config

    443/tcp - state:filtered - service:https

Wifi: Tenda_465F30

- BSSID: C8:3A:35:46:5F:30
- Channel: 6
- Encrypt: WPA2 WPA
- Password: *12345678* => Weak

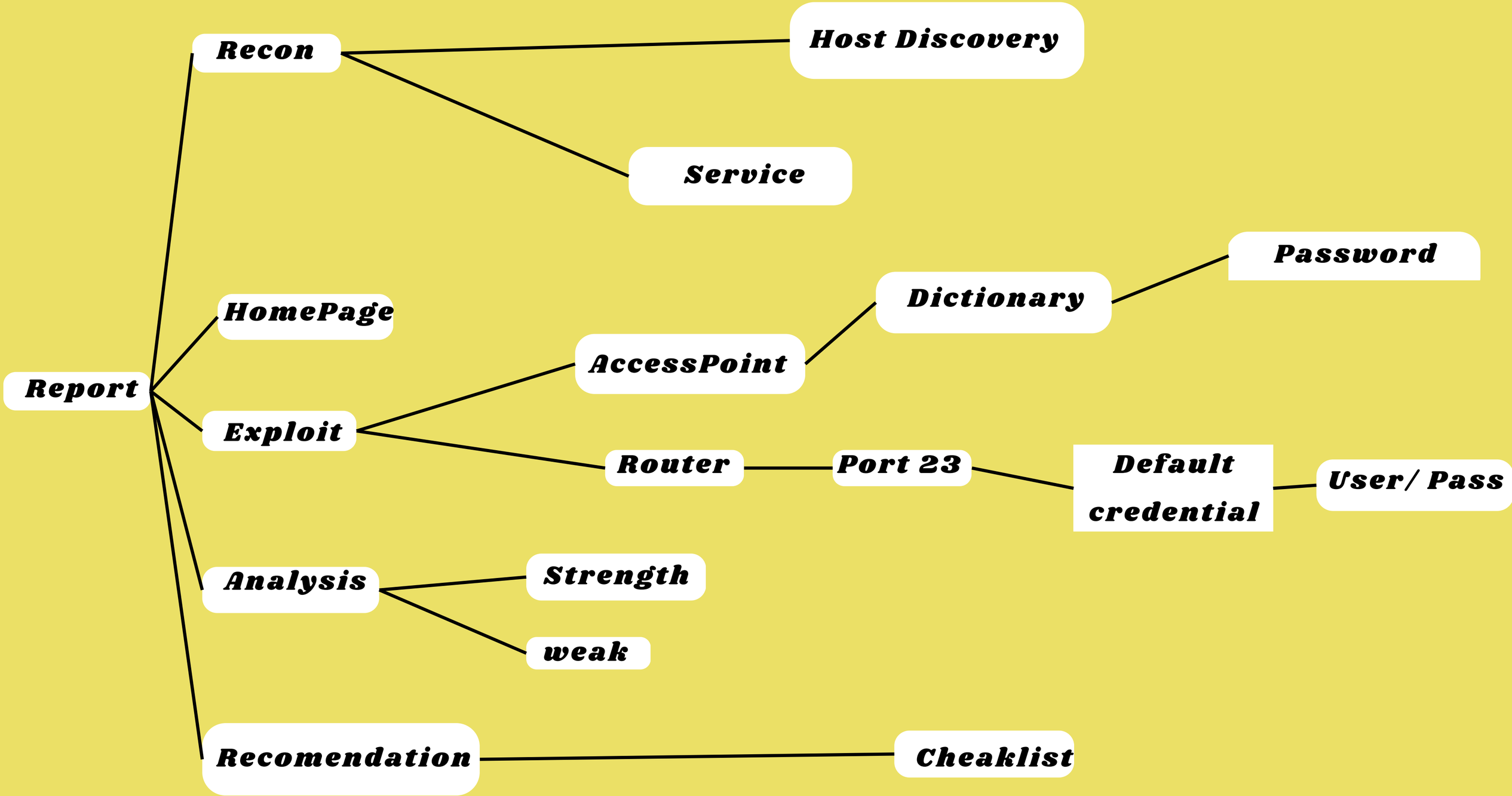
Router: 7200 Software (C7200-ADVENTERPRISEK9-M)

- IP: 192.168.1.1
- Version: 12.4(24)TS
- Vulnerability: Default Credentials Attack

+ Username : admin
+ Password : admin

Thank for listening!

PENNET TEAM


Report
Recon
Host Discovery
Service
HomePage
Exploit
AccessPoint
Dictionary
Password
Router
Port 23
Default credential
User/ Pass
Analysis
Strength
weak
Recomendation
Cheaklist