**Lab 2. Quét mạng (Scanning networks)**

Detect Ports, OSes, services, and vulnerabilities

**Submission:**

You will compose a lab report that documents each step you take, including screenshots to illustrate the effects of commands you type, and describing your observations. Simply attaching code without any explanation will not receive credits

**Time duration:** 1 week

Network Topology:



1. (2,5 đ) Using nmap to scan a machine (via IP address or name) to detect an OS & services

* Students can use some commands:

$ sudo nmap –F *<network> //replace <Network> with 192.168.12.0/24*

$ sudo nmap –O *<IP-target> //replace <IP-target> with 192.168.12.254*

$ sudo nmap –A *<IP-target>*

$ sudo nmap –sV *<IP-target>*

* Find the differences when using these commands with:
* **Turn off** the firewall on the target machine (192.168.12.254)
* **Turn on** the firewall on the target machine
* Students use some other options of the nmap to detect the target.

1. (2,5 đ) **Using nmap with vul-scrip to detect vulnerabilities on an OS**

**Step 1.** Install vul-scrip (to detect detailed vulnerabilities)

$git clone https://github.com/scipag/vulscan scipag\_vulscan

$sudo ln -s `pwd`/scipag\_vulscan /usr/share/nmap/scripts/vulscan

**Step 2.** Run with the command:

$sudo nmap -sV --script=vulscan/vulscan.nse *<IP-target>*

**Note:** see the website for more details: <https://securitytrails.com/blog/nmap-vulnerability-scan>

Sv chọn khoảng 5 lỗ hổng có mã CVE, tìm hiểu và giải thích lỗ hổng đó, ghi trong báo cáo.

1. (3,0 đ) **Khai thác lỗ hổng**

* Sử dụng chương trình Cain&Abel or Ettercap để sniff file username và password của máy Client
* Tiến hành crack password của các client với Cain&Abel
* Sử dụng metaploit để truy cập vào các máy với các lỗ hổng remote.

1. (2,0 đ) **Hướng khắc phục**

* Đưa ra hướng khắc phục để chống lại quá trình quét mạng của attacker