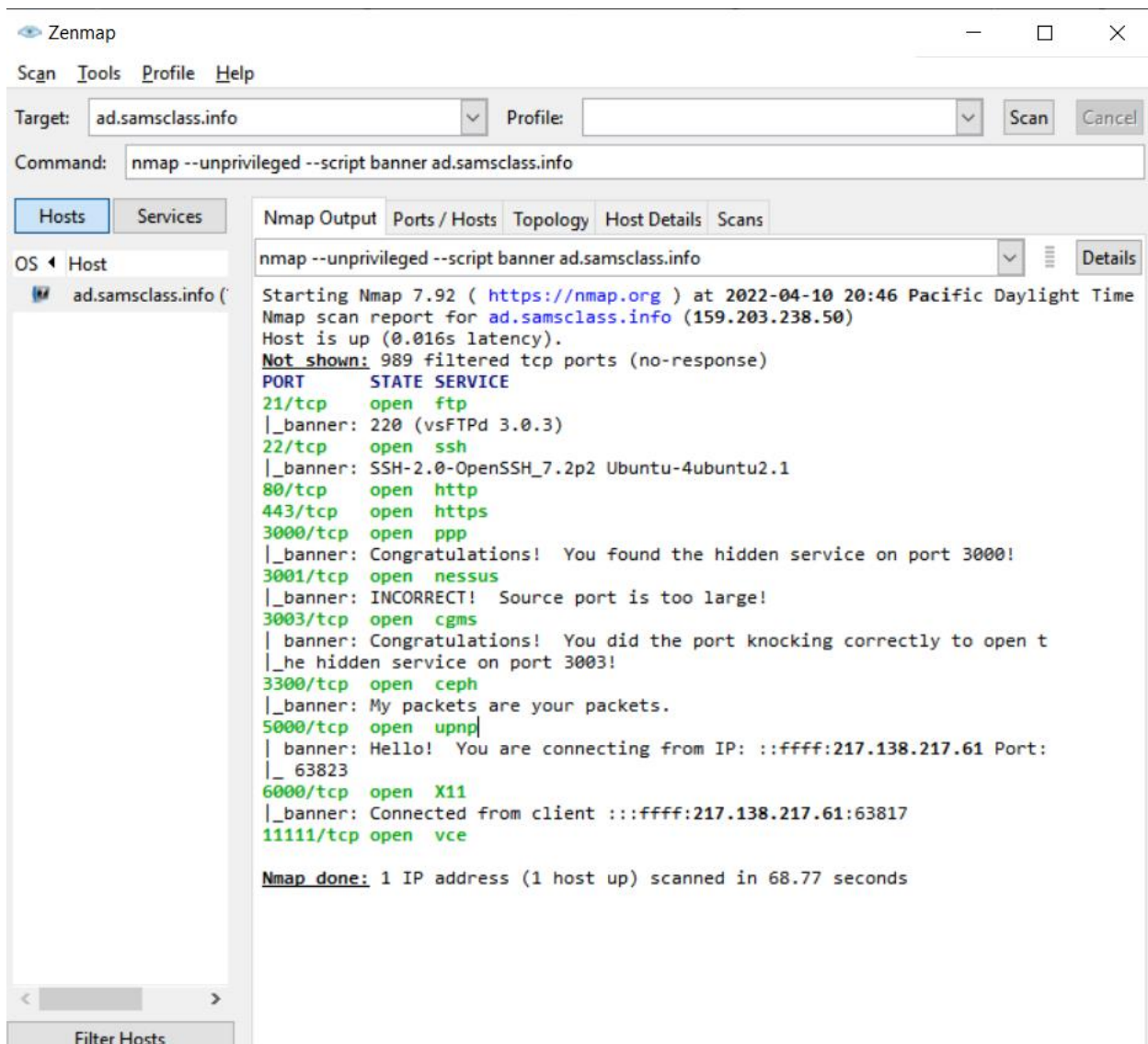


Flag H 131.1: Stolen Password

```
Ubuntu Server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
ig -p 2222 [listener] 0 of 10-100 startups
root      2998  0.0  0.7 13204 7944 ?        Ss   01:04   0:00 sshd: waldo [priv]
sshd      3006  0.0  0.4 12172 4640 ?        S    01:04   0:00 sshd: waldo [net]
ubuntu    3009  0.0  0.0  6432  724 tty1    S+   01:05   0:00 grep --color=auto ssh
ubuntu@techtools:~$ sudo strace -p 2998 2> foo
ubuntu@techtools:~$ sudo ps aux | grep ssh
root      703  0.0  0.7 12172 7540 ?        Ss   00:18   0:00 sshd: /usr/sbin/sshd -D [listener
] 1 of 10-100 startups
root      2972  0.0  0.2 12172 2960 ?        Ss   01:02   0:00 sshd: /usr/sbin/sshd -f sshd_conf
ig -p 2222 [listener] 0 of 10-100 startups
root      3016  0.1  0.8 13204 8016 ?        Ss   01:07   0:00 sshd: waldo [priv]
sshd      3017  0.0  0.4 12172 4688 ?        S    01:07   0:00 sshd: waldo [net]
ubuntu    3019  0.0  0.0  6432  656 tty1    S+   01:07   0:00 grep --color=auto ssh
ubuntu@techtools:~$ sudo strace -p 3016 2> foo
ubuntu@techtools:~$ sudo ps aux | grep ssh
root      703  0.0  0.7 12172 7540 ?        Ss   00:18   0:00 sshd: /usr/sbin/sshd -D [listener
] 1 of 10-100 startups
root      2972  0.0  0.2 12172 2960 ?        Ss   01:02   0:00 sshd: /usr/sbin/sshd -f sshd_conf
ig -p 2222 [listener] 0 of 10-100 startups
root      3027  0.5  0.8 13204 8180 ?        Ss   01:09   0:00 sshd: waldo [priv]
sshd      3028  0.0  0.4 12172 4584 ?        S    01:09   0:00 sshd: waldo [net]
ubuntu    3030  0.0  0.0  6432  720 tty1    S+   01:09   0:00 grep --color=auto ssh
ubuntu@techtools:~$ sudo strace -p 3027 2> foo

ubuntu@techtools:~$
ubuntu@techtools:~$ head foo
strace: Process 3027 attached
restart_syscall(<... resuming interrupted read ...>) = 1
read(6, "\0\0\0\0", 4) = 4
read(6, "\f\0\0\0\07cecsMJZ", 12) = 12
getuid() = 0
openat(AT_FDCWD, "/etc/login.defs", O_RDONLY) = 5
fstat(5, {st_mode=S_IFREG|0644, st_size=10550, ...}) = 0
read(5, "#\n# /etc/login.defs - Configurat"... , 4096) = 4096
read(5, " issuing \n# the \"msg y\" command"... , 4096) = 4096
read(5, "algorithm compatible with the on"... , 4096) = 2358
ubuntu@techtools:~$ _
```

H 410.2: My packets



Zenmap

Scan Tools Profile Help

Target: Profile: Scan Cancel

Command:

Hosts Services

OS Host

ad.samsclass.info (

Nmap Output Ports / Hosts Topology Host Details Scans

nmap --unprivileged --script banner ad.samsclass.info Details

Starting Nmap 7.92 (<https://nmap.org>) at 2022-04-10 20:46 Pacific Daylight Time
Nmap scan report for ad.samsclass.info (159.203.238.50)
Host is up (0.016s latency).
Not shown: 989 filtered tcp ports (no-response)

PORT	STATE	SERVICE
21/tcp	open	ftp
_banner: 220 (vsFTPD 3.0.3)		
22/tcp	open	ssh
_banner: SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.1		
80/tcp	open	http
443/tcp	open	https
3000/tcp	open	ppp
_banner: Congratulations! You found the hidden service on port 3000!		
3001/tcp	open	nessus
_banner: INCORRECT! Source port is too large!		
3003/tcp	open	cgms
_banner: Congratulations! You did the port knocking correctly to open t		
_he hidden service on port 3003!		
3300/tcp	open	ceph
_banner: My packets are your packets.		
5000/tcp	open	upnp
_banner: Hello! You are connecting from IP: ::ffff:217.138.217.61 Port:		
_ 63823		
6000/tcp	open	X11
_banner: Connected from client :::ffff:217.138.217.61:63817		
11111/tcp	open	vce

Nmap done: 1 IP address (1 host up) scanned in 68.77 seconds

Filter Hosts

Port 3300

H 410.3: Key to the universe

cript banner ad.samsclass.info

```
Nmap Output  Ports / Hosts  Topology  Host Details  Scans
nmap -p 11223 --unprivileged --script banner ad.samsclass.info

Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-10 23:04 Pacific Daylight Time
Nmap scan report for ad.samsclass.info (159.203.238.50)
Host is up (0.018s latency).

PORT      STATE SERVICE
11223/tcp  open  unknown
|_banner: The key to the Universe.

Nmap done: 1 IP address (1 host up) scanned in 16.61 seconds
```

This one was hard, I couldn't find the port, so I exploited a loophole

Using the previous scan, I went into the tables that showed the available ports that were scanned in the nmap scan. I then brute-forced the answer input on the website provided to check our answers until I got the right port. To make sure it was correct for me and for practice with the nmap commands, I ran the above command. This also serves as my proof. I don't know why, however, if I tried to run the command to scan all the available ports on the server, why this specific port didn't show up, maybe it was one of the filtered ports.

Port 11223