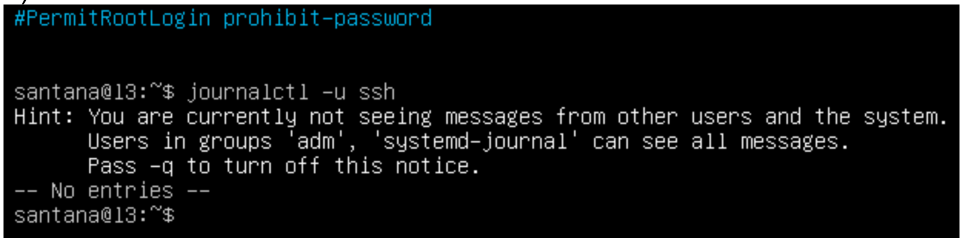
Turn In lab 10 – Ethan Roepke

1. **Submit a screenshot of the SSH brute force you performed from Lab 04.**
   (5 points)



```
#PermitRootLogin prohibit-password


santana@l3:~$ journalctl -u ssh
Hint: You are currently not seeing messages from other users and the system.
      Users in groups 'adm', 'systemd-journal' can see all messages.
      Pass -q to turn off this notice.
-- No entries --
santana@l3:~$
```

2. Take a moment and list three potential services/options that could be configured to help mitigate brute-force attacks and why

(5 points)

MaxAuthTries: the default number it is set to is 6, however if we lower this number, the likelihood of a brute force attack will be less effective because it limits the number of authentications attempts per user.

LoginGraceTime: having the LoginGraceTime at a lower timer will terminate the connection for being authenticated. Having at a low time will prevent brute attacks significantly.

PermitRootLogin: This options decides if they get root on login or if the root user needs to authenticate them through a non root user. This will make brute attack less effective as they would have to authenticate under non root user.

3. Explain two additional methods we can use to prevent brute force attacks. Be specific.

(5 points)

Strong password policies: Implementing password policies such as: minimum characters, uppercase/lowercase, and numbers/special characters which will be more resistant to brute force attacks as it will be harder to guess the password. We could implement a required password change very so often to keep passwords updated.

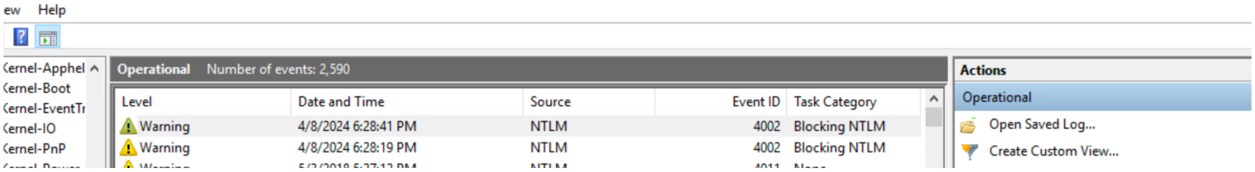
Authentication limit per IP: being able to restrict the number of authentication attempts from a specific IP and blocking that IP will help mitigate brute force attacks. We have tools such as IPTables that will automatically block IP addresses that fail 'x' amount of login tries.

4. What does Event ID 4672 mean? What privileges are assigned to somebody who logs in under this action? Be specific, no less than five sentences.

(5 points)

Event id 4672 is a special privilege assigned to new logon. The user will be granted privileges in one or more groups. The event will be logged when a user's group privilege is changed on the specific system such as being added/removed from a group or the permissions were modified. Somebody who logs in under this action would either have administrative access which would have full access and as well other groups below administrative.

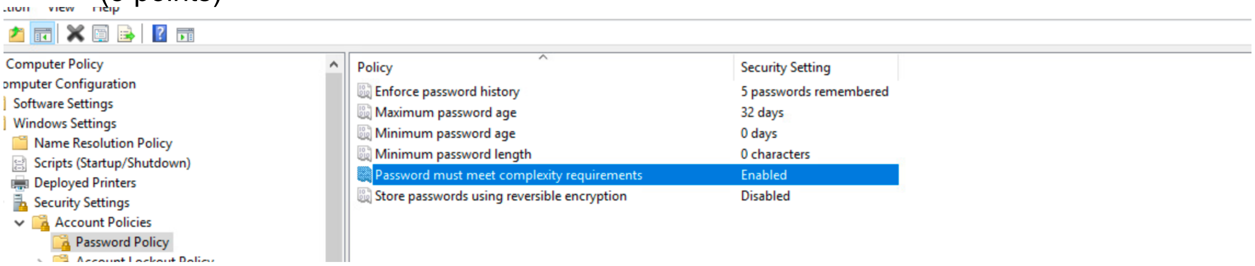
5. Take a screenshot of the failed NTLM login in Windows Event Viewer. What is the Event ID (four-digit0 code) of the failed login
(5 points)



Operational Number of events: 2,590

Level	Date and Time	Source	Event ID	Task Category
Warning	4/8/2024 6:28:41 PM	NTLM	4002	Blocking NTLM
Warning	4/8/2024 6:28:19 PM	NTLM	4002	Blocking NTLM

6. Screenshot of modified password policy
(5 points)

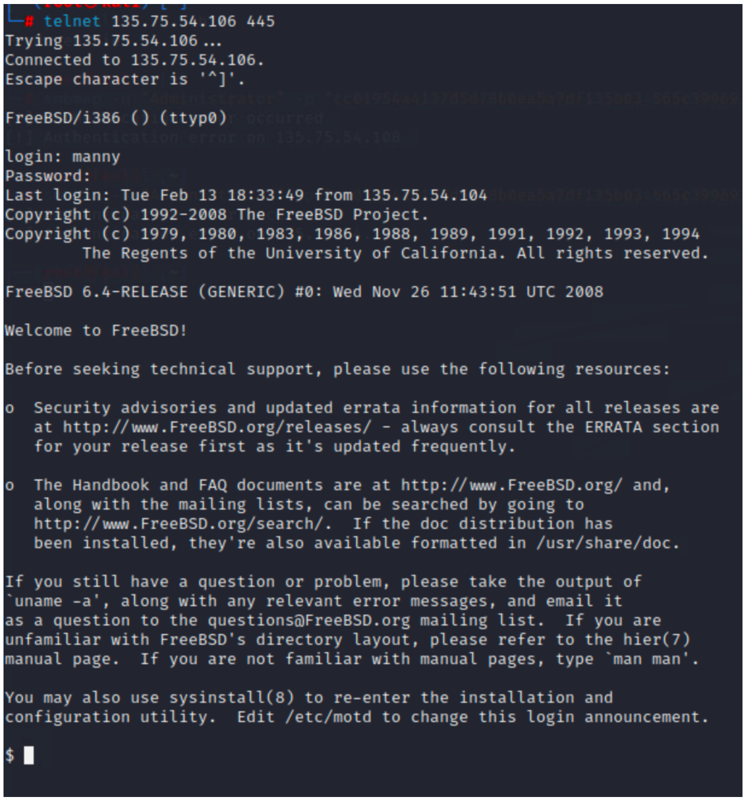


Policy	Security Setting
Enforce password history	5 passwords remembered
Maximum password age	32 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

7. What are the "complexity requirements" that we have enforced?
(5 points)

The complexity requirements that are enforced if enabled means the password must meet certain minimum requirements. This includes not including users full/part of users account name, at least 6 characters, and include 3 of these 4 options(capital letter, lowercase letter, number from 0-9, and special character).

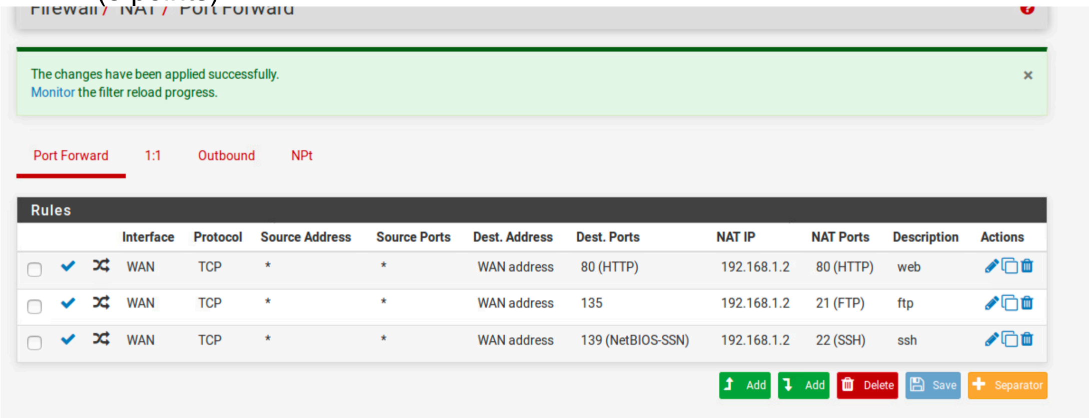
8. Screenshot of successful telnet login
(5 points)



```
└─# telnet 135.75.54.106 445
Trying 135.75.54.106 ...
Connected to 135.75.54.106.
Escape character is '^]'.

FreeBSD/i386 () (ttyp0)

login: manny
Password:
Last login: Tue Feb 13 18:33:49 from 135.75.54.104
Copyright (c) 1992-2008 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.

FreeBSD 6.4-RELEASE (GENERIC) #0: Wed Nov 26 11:43:51 UTC 2008

Welcome to FreeBSD!

Before seeking technical support, please use the following resources:

o   Security advisories and updated errata information for all releases are
    at http://www.FreeBSD.org/releases/ - always consult the ERRATA section
    for your release first as it's updated frequently.

o   The Handbook and FAQ documents are at http://www.FreeBSD.org/ and,
    along with the mailing lists, can be searched by going to
    http://www.FreeBSD.org/search/.  If the doc distribution has
    been installed, they're also available formatted in /usr/share/doc.

If you still have a question or problem, please take the output of
`uname -a', along with any relevant error messages, and email it
as a question to the questions@FreeBSD.org mailing list.  If you are
unfamiliar with FreeBSD's directory layout, please refer to the hier(7)
manual page.  If you are not familiar with manual pages, type `man man'.

You may also use sysinstall(8) to re-enter the installation and
configuration utility.  Edit /etc/motd to change this login announcement.

$ █
```

9. Screenshot of updated pfSense port-forwarding rules

(5 points)



Firewall / NAT / Port Forward

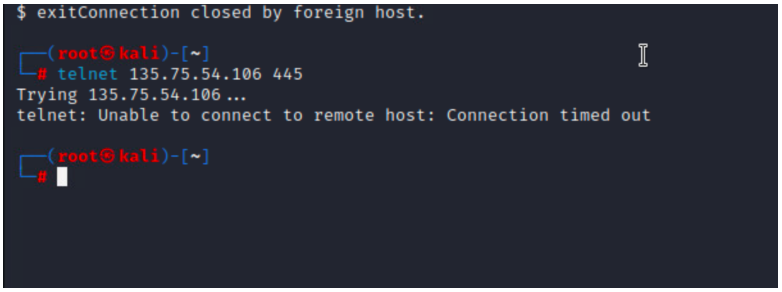
The changes have been applied successfully.
Monitor the filter reload progress.

Rules

			Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
□	✓	⤨	WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.1.2	80 (HTTP)	web	
□	✓	⤨	WAN	TCP	*	*	WAN address	135	192.168.1.2	21 (FTP)	ftp	
□	✓	⤨	WAN	TCP	*	*	WAN address	139 (NetBIOS-SSN)	192.168.1.2	22 (SSH)	ssh	

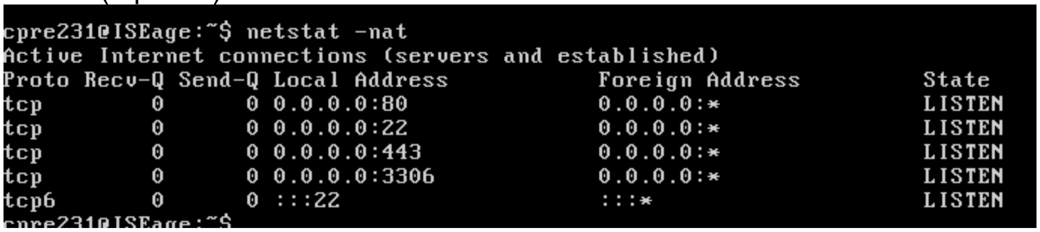
10. Screenshot of failed telnet login

(5 points)



```
$ exitConnection closed by foreign host.

┌──(root㉿kali)-[~]
└─# telnet 135.75.54.106 445
Trying 135.75.54.106 ...
telnet: Unable to connect to remote host: Connection timed out

┌──(root㉿kali)-[~]
└─# 
```

**11.	Screenshot of listening ports on XX.XX.XX.104**
(5 points)

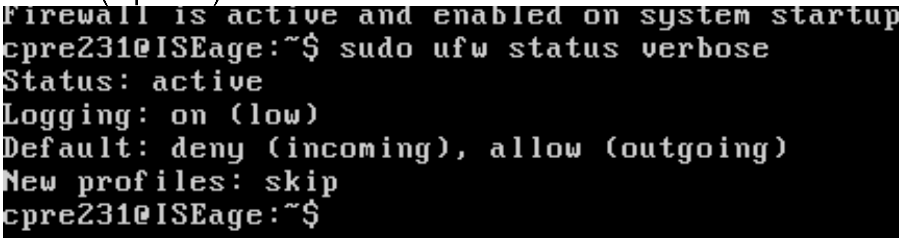


```
cpre231@ISEage:~$ netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
cpre231@ISEage:~$
```

**12.	What service is running at port 3306?**
(5 points)

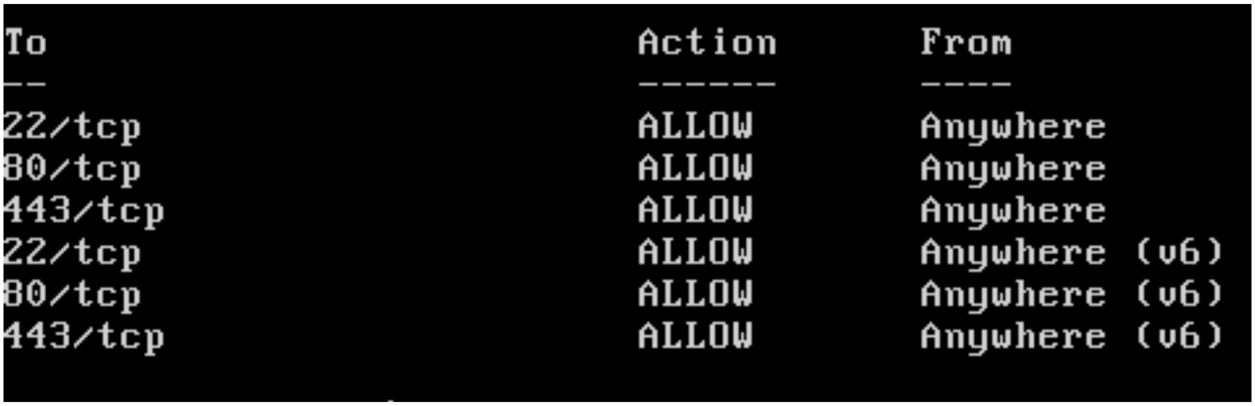
Port 3306 is associated with MySQL protocol. This port is used to connect to MySQL clients and utilities such as mysqldump.

**13.	Screenshot of default incoming/outgoing UFW policies**
(5 points)



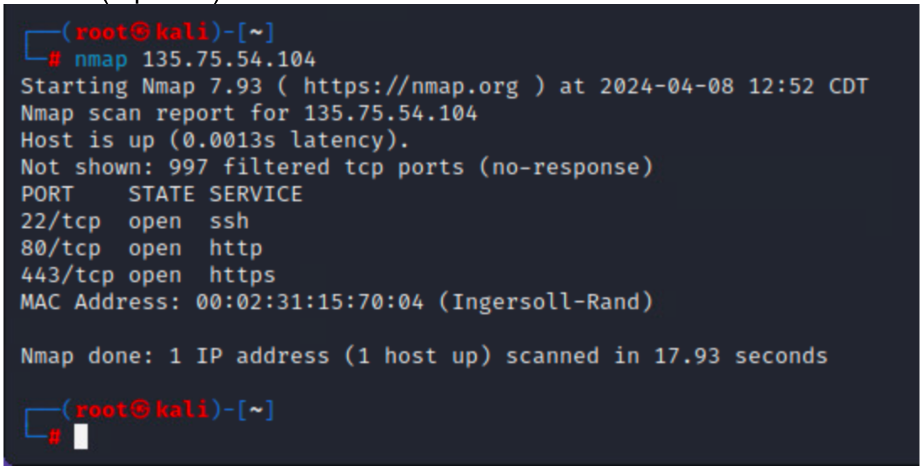
```
Firewall is active and enabled on system startup
cpre231@ISEage:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing)
New profiles: skip
cpre231@ISEage:~$
```

**14.	Screenshot of newly created UFW rules**
(5 points)



```
To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
80/tcp                     ALLOW       Anywhere
443/tcp                    ALLOW       Anywhere
22/tcp                     ALLOW       Anywhere (v6)
80/tcp                     ALLOW       Anywhere (v6)
443/tcp                    ALLOW       Anywhere (v6)
```

15. **Screenshot of nmap scan results showing blocked port 3306**
(5 points)

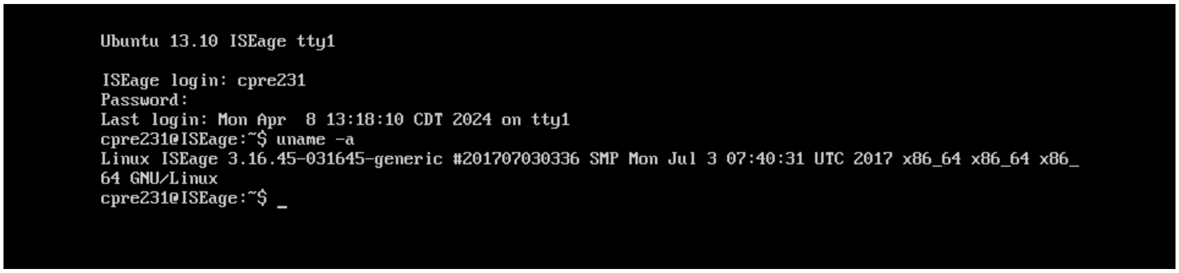


```
┌──(root㉿kali)-[~]
└─# nmap 135.75.54.104
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-08 12:52 CDT
Nmap scan report for 135.75.54.104
Host is up (0.0013s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
MAC Address: 00:02:31:15:70:04 (Ingersoll-Rand)

Nmap done: 1 IP address (1 host up) scanned in 17.93 seconds

┌──(root㉿kali)-[~]
└─# 
```

16. **Specify which domain these packages are being downloaded from. Why?**
(5 points)

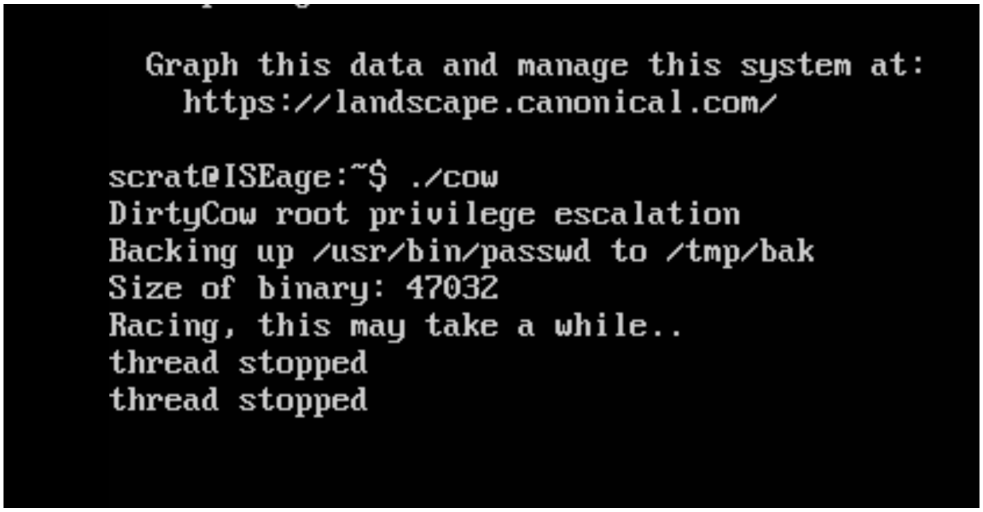
These packages are being downloaded from the domain “ubuntu”. We had to get the deb files from ubuntu to make sure the deb files are stable with other OS that are used with ubuntu, easy to install through ubuntu, and for a level of security to address vulnerabilities and bugs.

17. **Screenshot of upgraded kernel version**
(10 points)



```
Ubuntu 13.10 ISEage tty1

ISEage login: cpre231
Password:
Last login: Mon Apr  8 13:18:10 CDT 2024 on tty1
cpre231@ISEage:~$ uname -a
Linux ISEage 3.16.45-031645-generic #201707030336 SMP Mon Jul 3 07:40:31 UTC 2017 x86_64 x86_64 x86_
64 GNU/Linux
cpre231@ISEage:~$ _
```

**18.	Screenshot of “hung” Dirty Cow**
(5 points)



```
  Graph this data and manage this system at:
    https://landscape.canonical.com/

scrat@ISEage:~$ ./cow
DirtyCow root privilege escalation
Backing up /usr/bin/passwd to /tmp/bak
Size of binary: 47032
Racing, this may take a while..
thread stopped
thread stopped
```

**19.	Number of versions will you have to upgrade through from 13.10 to the current LTS**

(5 points)

5 versions