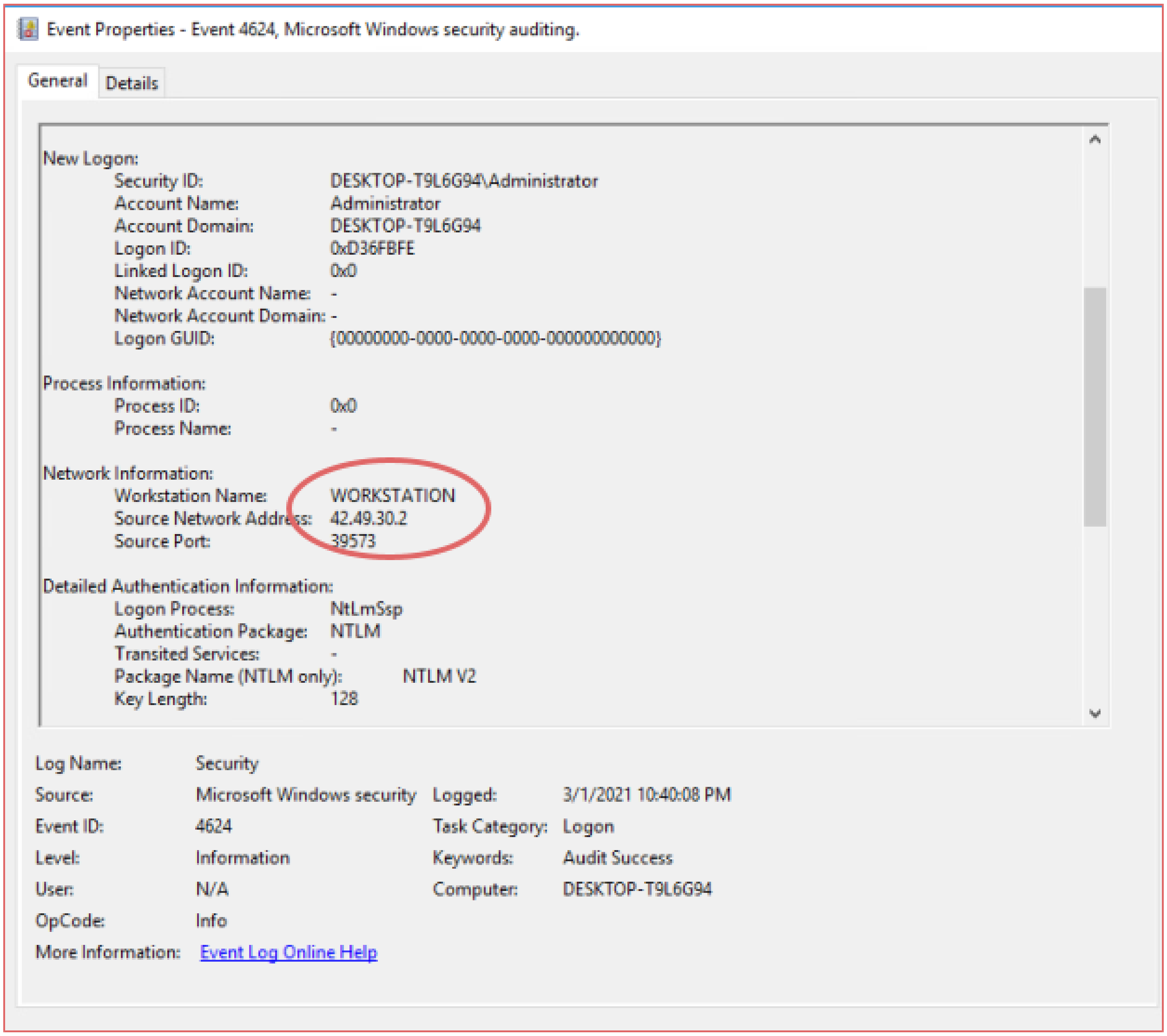
1. Screenshot of successful NTLM login in Windows Event Viewer
    a. Where did this login originate from? IP and Machine Name

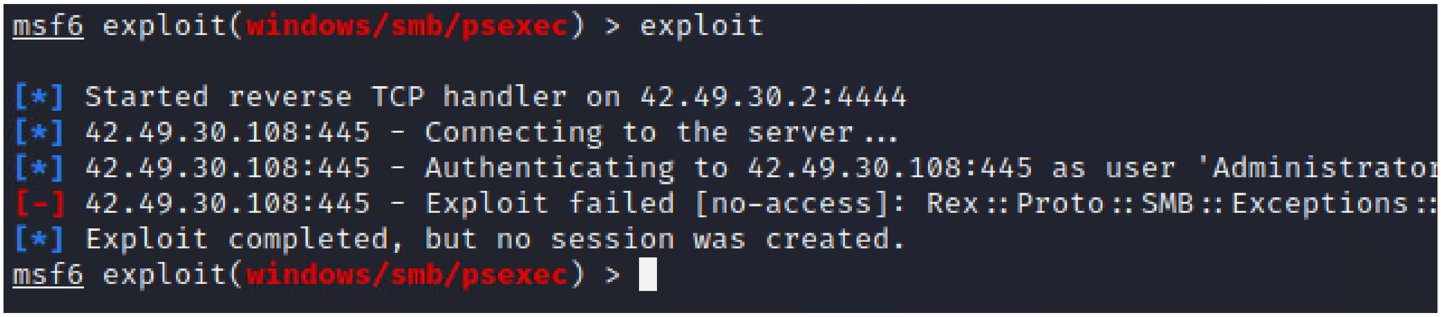


Event Properties - Event 4624, Microsoft Windows security auditing.
General
Details

```
New Logon:
        Security ID:                DESKTOP-T9L6G94\Administrator
        Account Name:               Administrator
        Account Domain:             DESKTOP-T9L6G94
        Logon ID:                   0xD36FBFE
        Linked Logon ID:            0x0
        Network Account Name:       -
        Network Account Domain:     -
        Logon GUID:                 {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:                 0x0
        Process Name:               -

Network Information:
        Workstation Name:           WORKSTATION
        Source Network Address:     42.49.30.2
        Source Port:                39573

Detailed Authentication Information:
        Logon Process:              NtLmSsp
        Authentication Package:     NTLM
        Transited Services:         -
        Package Name (NTLM only):           NTLM V2
        Key Length:                 128
```

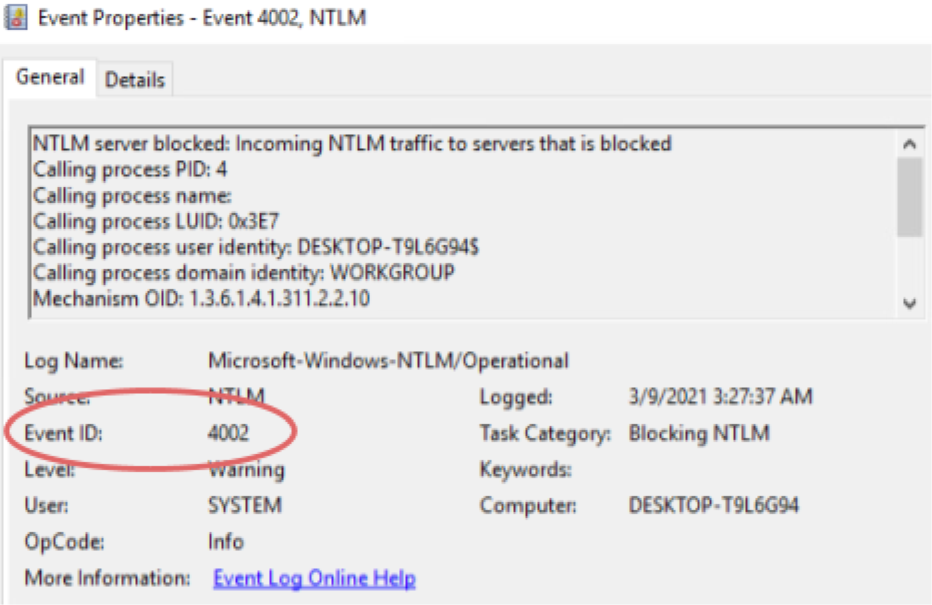
Log Name:	Security		
Source:	Microsoft Windows security	Logged:	3/1/2021 10:40:08 PM
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DESKTOP-T9L6G94
OpCode:	Info		
More Information:	Event Log Online Help		

2. Screenshot of failed psexec attempt in Kali



```
msf6 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 42.49.30.2:4444
[*] 42.49.30.108:445 - Connecting to the server...
[*] 42.49.30.108:445 - Authenticating to 42.49.30.108:445 as user 'Administrator
[-] 42.49.30.108:445 - Exploit failed [no-access]: Rex::Proto::SMB::Exceptions::
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/psexec) > 
```

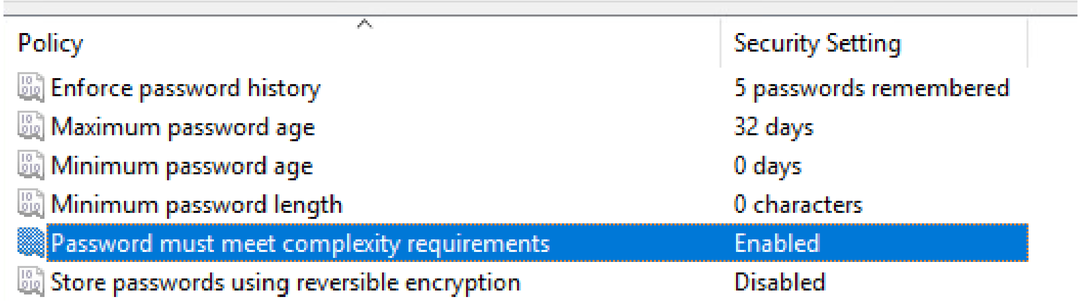
3. Screenshot of failed NTLM login in Windows Event Viewer
    a. What is the Event ID?



```
NTLM server blocked: Incoming NTLM traffic to servers that is blocked
Calling process PID: 4
Calling process name:
Calling process LUID: 0x3E7
Calling process user identity: DESKTOP-T9L6G94$
Calling process domain identity: WORKGROUP
Mechanism OID: 1.3.6.1.4.1.311.2.2.10
```

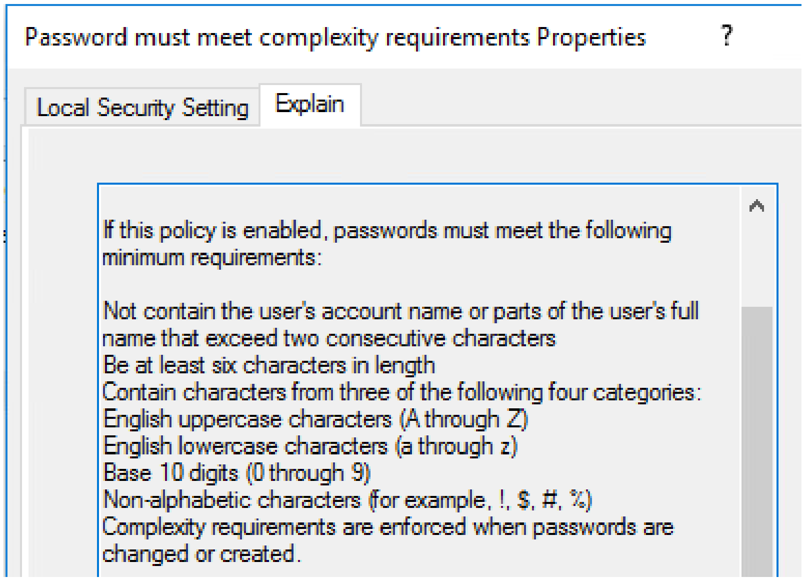
Log Name: Microsoft-Windows-NTLM/Operational
Source: NTLM
Logged: 3/9/2021 3:27:37 AM
Event ID: 4002
Task Category: Blocking NTLM
Level: Warning
Keywords:
User: SYSTEM
Computer: DESKTOP-T9L6G94
OpCode: Info
More Information: Event Log Online Help

4. Screenshot of modified password policy changed as specified in lab



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

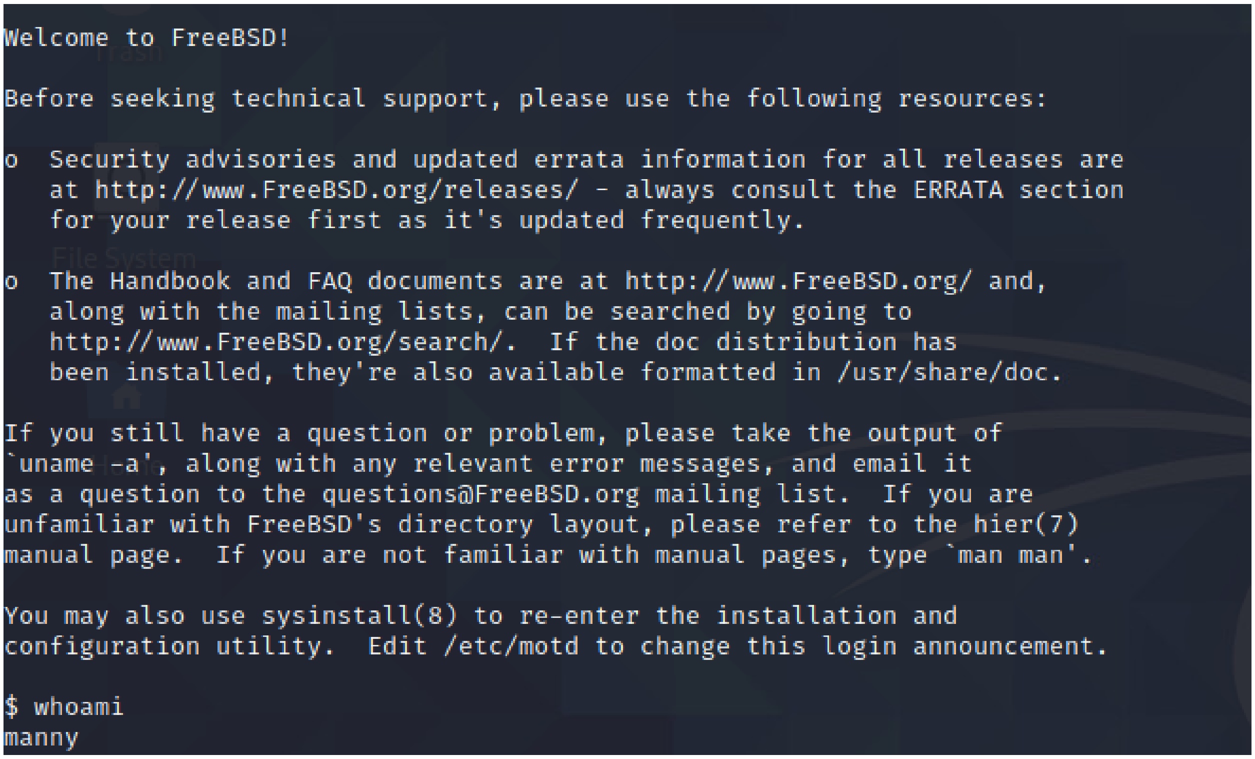
    a. What are the "complexity requirements" that we have enforced?



If this policy is enabled, passwords must meet the following minimum requirements:

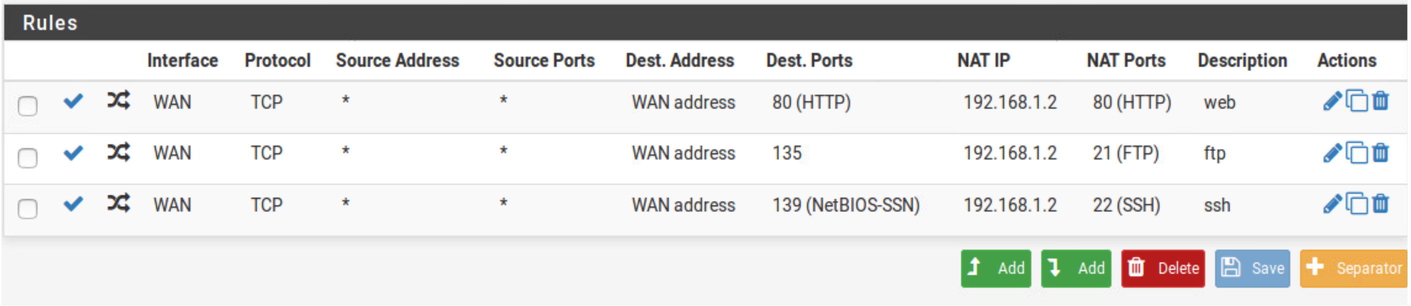
Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
Be at least six characters in length
Contain characters from three of the following four categories:
English uppercase characters (A through Z)
English lowercase characters (a through z)
Base 10 digits (0 through 9)
Non-alphabetic characters (for example, !, $, #, %)
Complexity requirements are enforced when passwords are changed or created.

5. Screenshot of successful telnet login



```
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.

$ whoami
manny
```

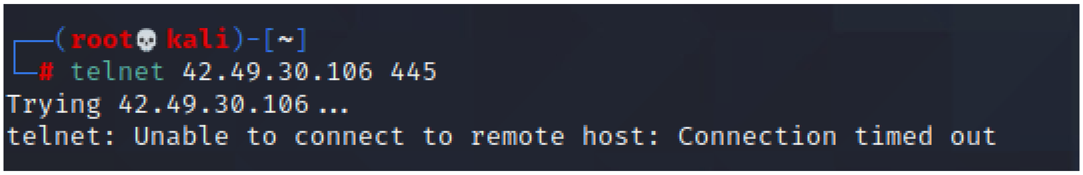
6. Screenshot of updated pfSense port-forwarding rules



Rules

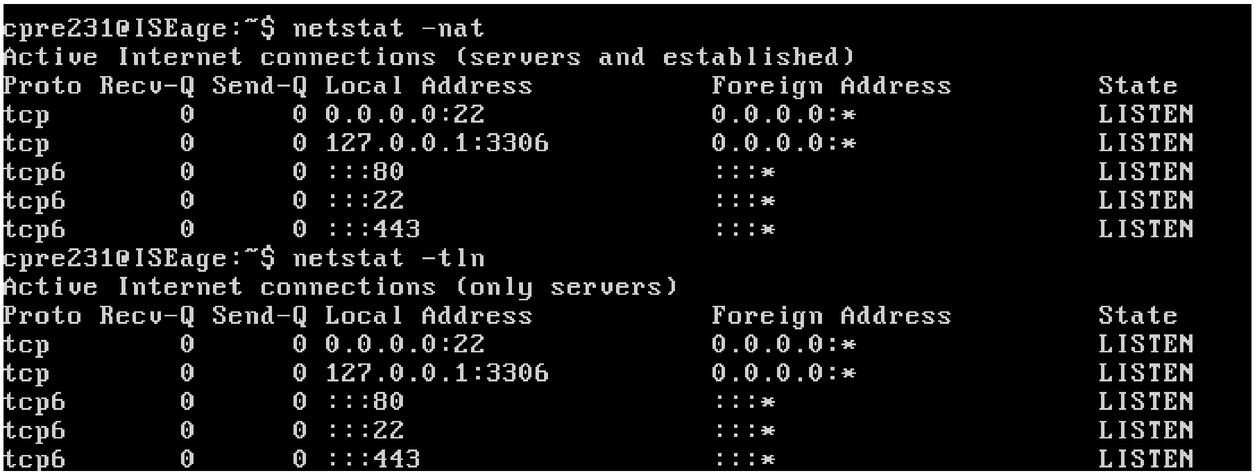
			Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
□	✓	⤮	WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.1.2	80 (HTTP)	web	✎ ⧉ 🗑
□	✓	⤮	WAN	TCP	*	*	WAN address	135	192.168.1.2	21 (FTP)	ftp	✎ ⧉ 🗑
□	✓	⤮	WAN	TCP	*	*	WAN address	139 (NetBIOS-SSN)	192.168.1.2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

7. Screenshot of denied telnet login



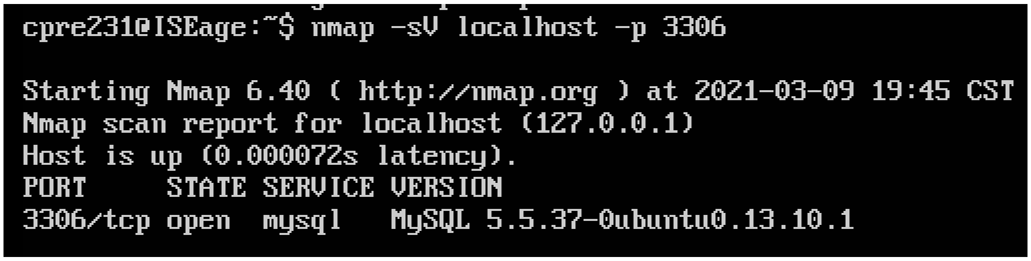
```
┌──(root💀kali)-[~]
└─# telnet 42.49.30.106 445
Trying 42.49.30.106...
telnet: Unable to connect to remote host: Connection timed out
```

8. Screenshot of listening ports on XX.XX.XX.104 (netstat -nat and -tln)



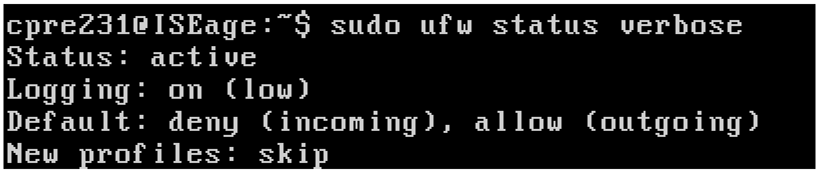
```
cpre231@ISEage:~$ netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::443                  :::*                    LISTEN
cpre231@ISEage:~$ netstat -tln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::443                  :::*                    LISTEN
```

9. What service is running at port 3306? (Didn't picture until after update to 13.10)



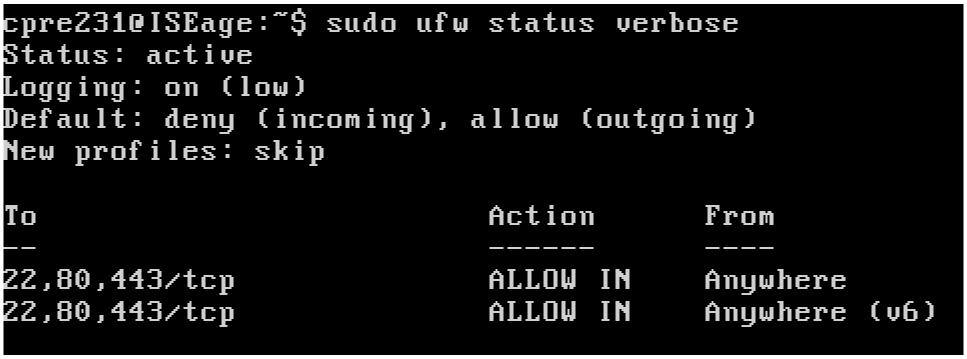
```
cpre231@ISEage:~$ nmap -sV localhost -p 3306

Starting Nmap 6.40 ( http://nmap.org ) at 2021-03-09 19:45 CST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000072s latency).
PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL 5.5.37-0ubuntu0.13.10.1
```

10. Screenshot of default incoming/outgoing UFW policies



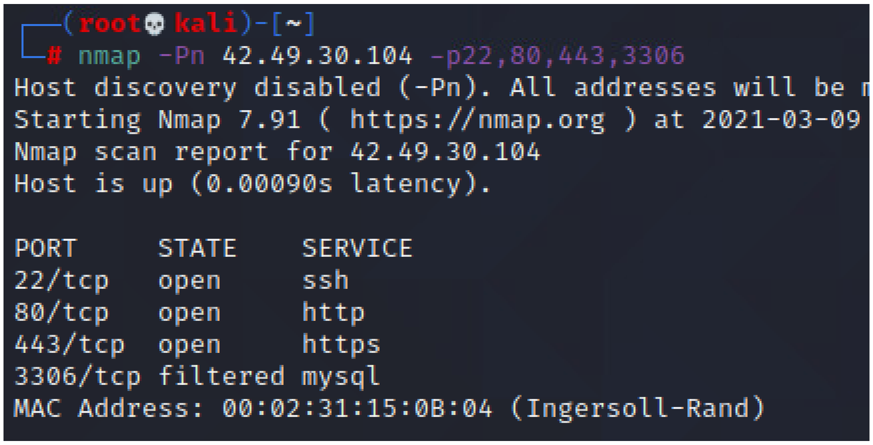
```
cpre231@ISEage:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing)
New profiles: skip
```

11. Screenshot of newly created UFW rules



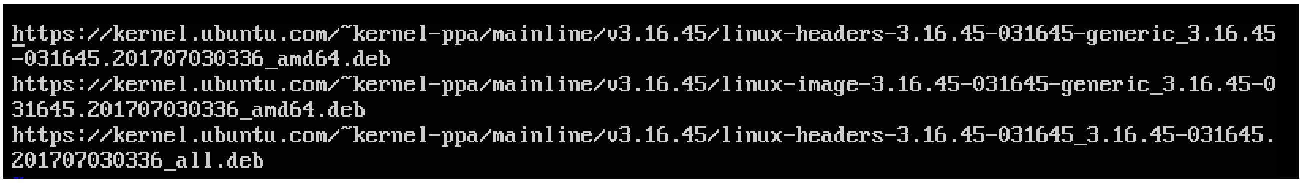
```
cpre231@ISEage:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing)
New profiles: skip

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

12. Screenshot of nmap scan results showing blocked port 3306



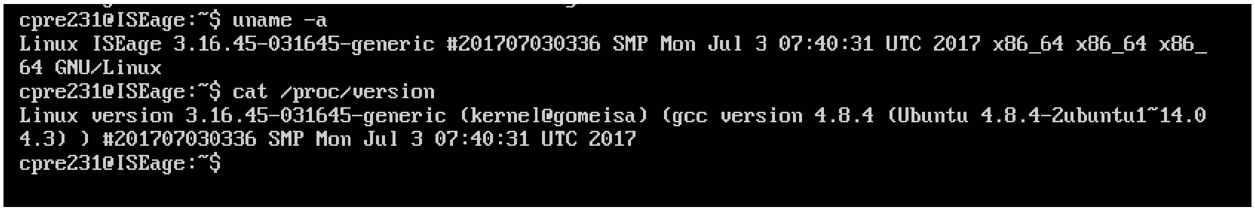
```
┌──(root💀kali)-[~]
└─# nmap -Pn 42.49.30.104 -p22,80,443,3306
Host discovery disabled (-Pn). All addresses will be m
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-09
Nmap scan report for 42.49.30.104
Host is up (0.00090s latency).

PORT     STATE    SERVICE
22/tcp   open     ssh
80/tcp   open     http
443/tcp  open     https
3306/tcp filtered mysql
MAC Address: 00:02:31:15:0B:04 (Ingersoll-Rand)
```

13. Specify which domain these packages are being downloaded from: **kernel.ubuntu.com**



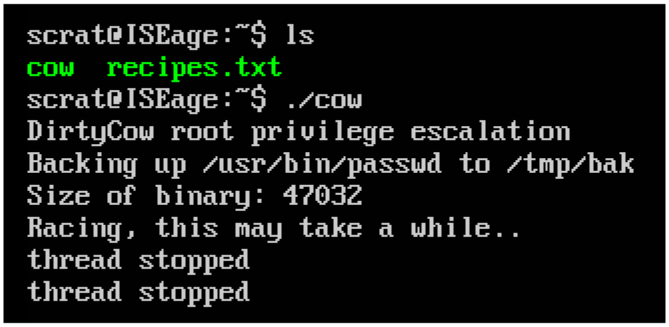
```
https://kernel.ubuntu.com/~kernel-ppa/mainline/v3.16.45/linux-headers-3.16.45-031645-generic_3.16.45
-031645.201707030336_amd64.deb
https://kernel.ubuntu.com/~kernel-ppa/mainline/v3.16.45/linux-image-3.16.45-031645-generic_3.16.45-0
31645.201707030336_amd64.deb
https://kernel.ubuntu.com/~kernel-ppa/mainline/v3.16.45/linux-headers-3.16.45-031645_3.16.45-031645.
201707030336_all.deb
```

14. Screenshot of upgraded kernel version (uname -a and /proc/version)



```
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:~$ cat /proc/version
Linux version 3.16.45-031645-generic (kernel@gomeisa) (gcc version 4.8.4 (Ubuntu 4.8.4-2ubuntu1~14.0
4.3) ) #201707030336 SMP Mon Jul 3 07:40:31 UTC 2017
cpre231@ISEage:~$
```

15. Screenshot of “hung” Dirty Cow



```
scrat@ISEage:~$ ls
cow  recipes.txt
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
```

16. Number of versions will you have to upgrade through from 13.10 to 20.04 LTS
Tree : 12.10 -> 13.10 -> 14.04 -> 16.04 -> 18.04 -> 20.04
Four more times. (All with a high risk of breaking something.)