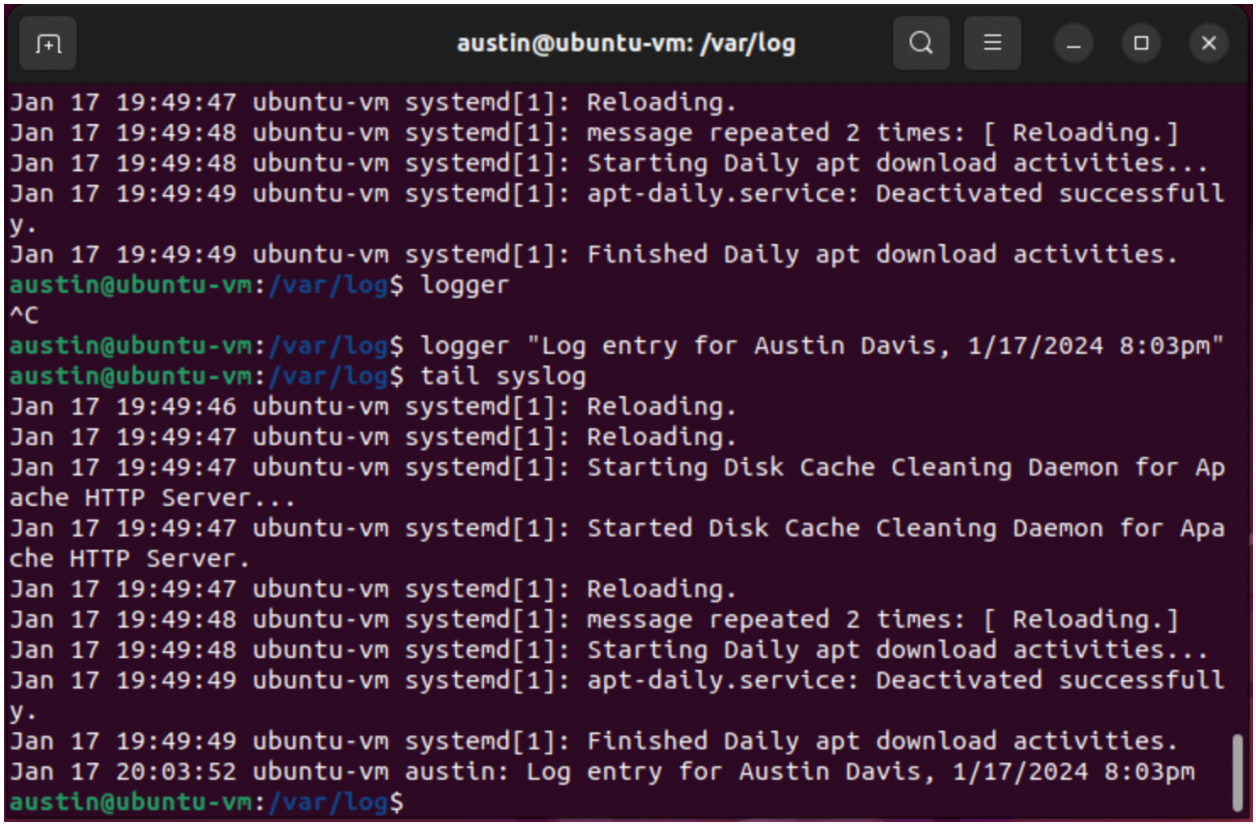
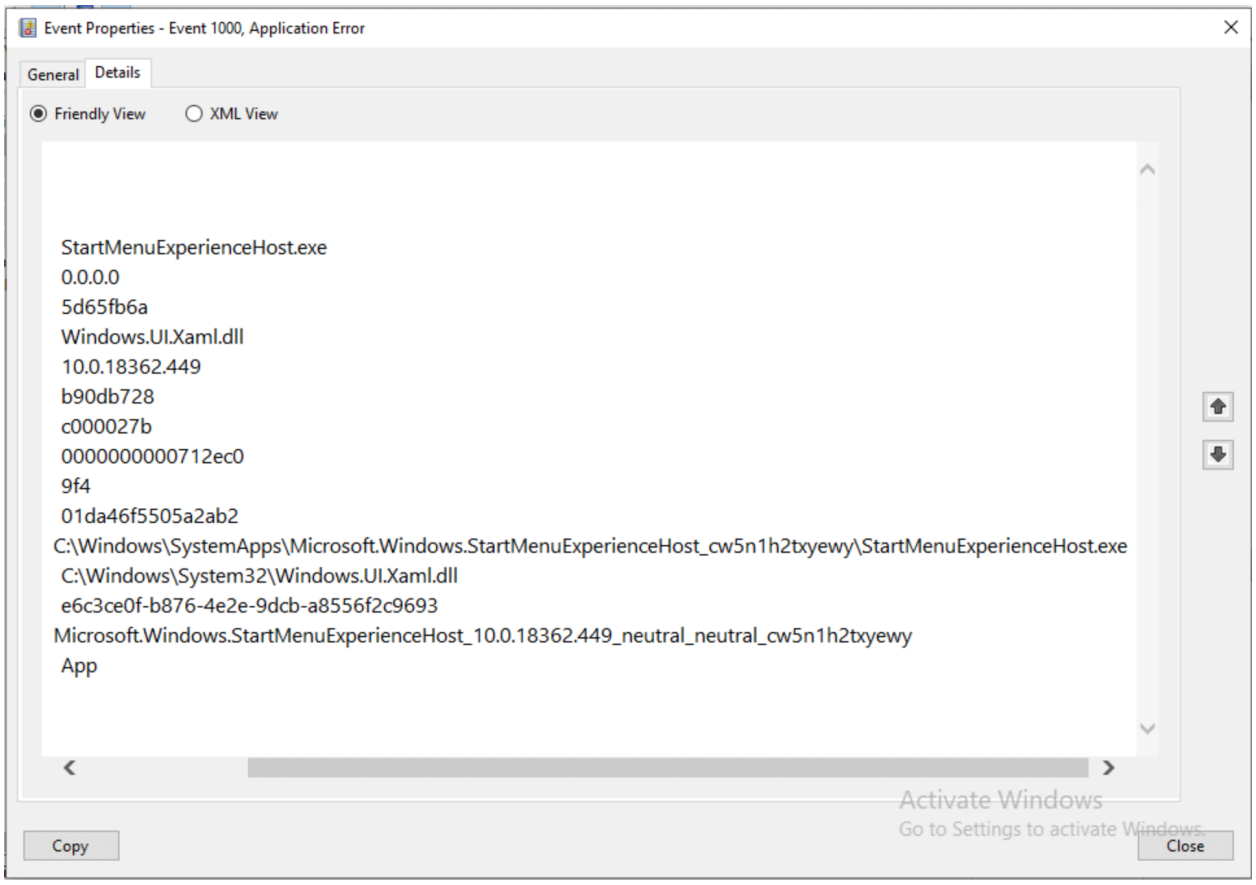
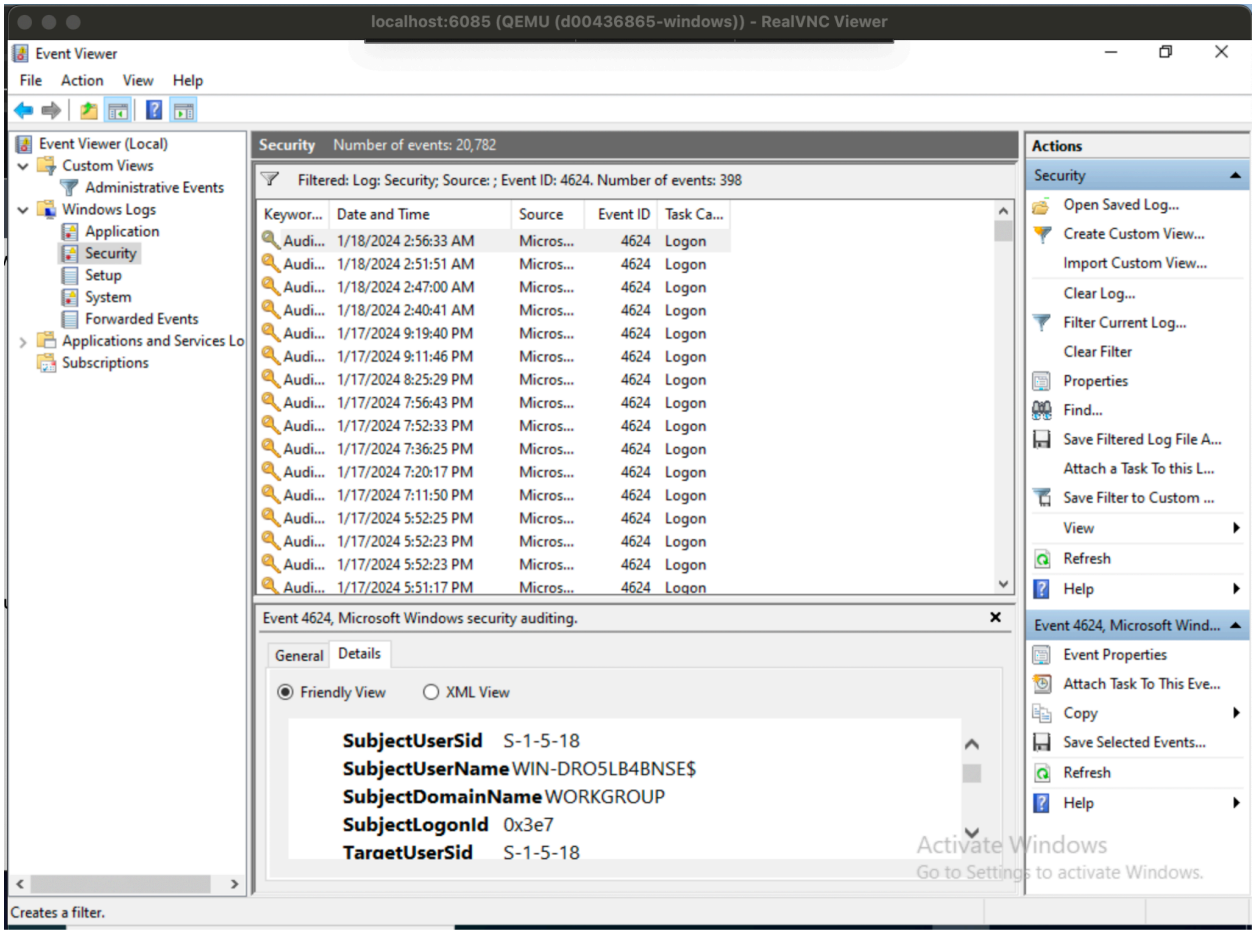
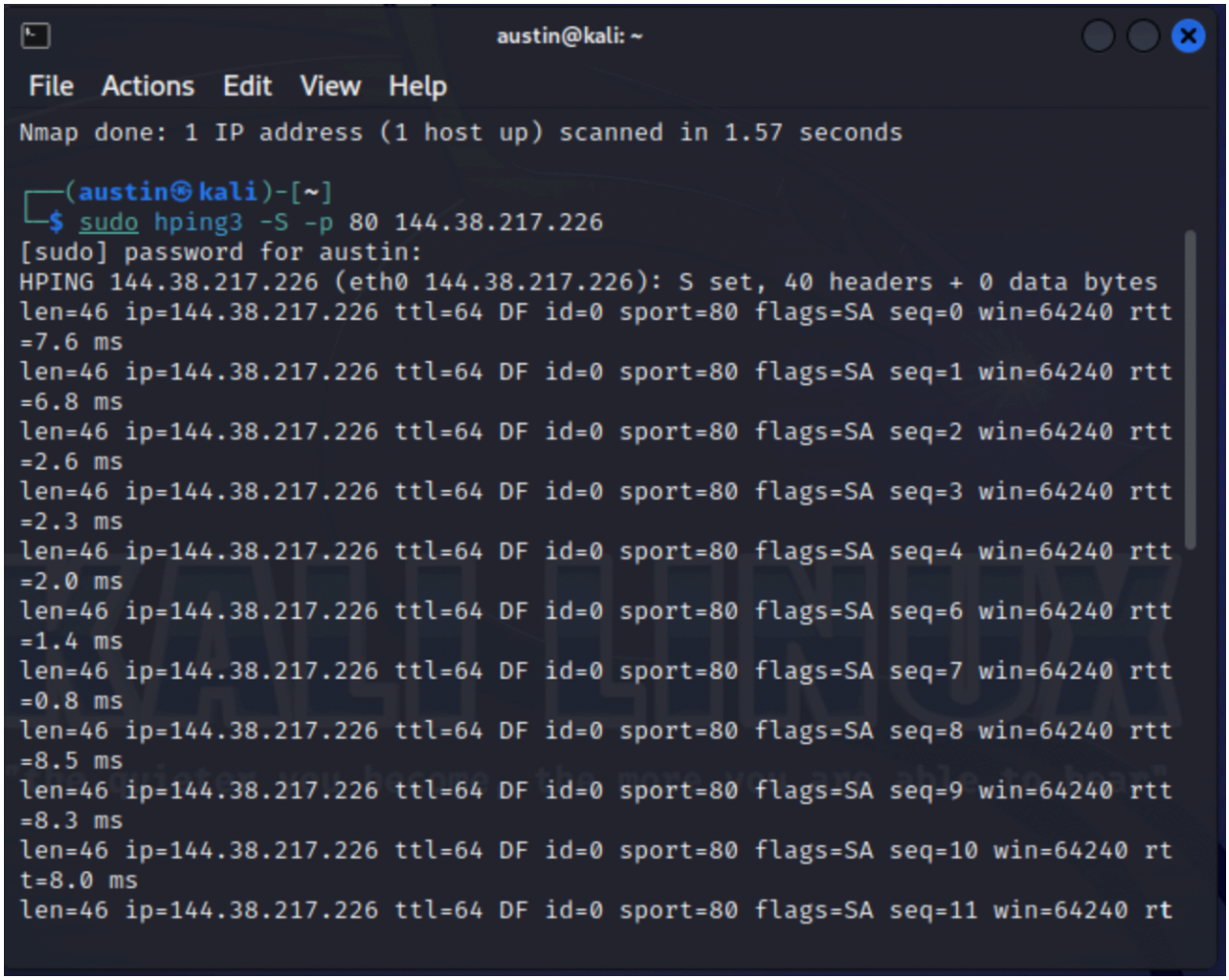
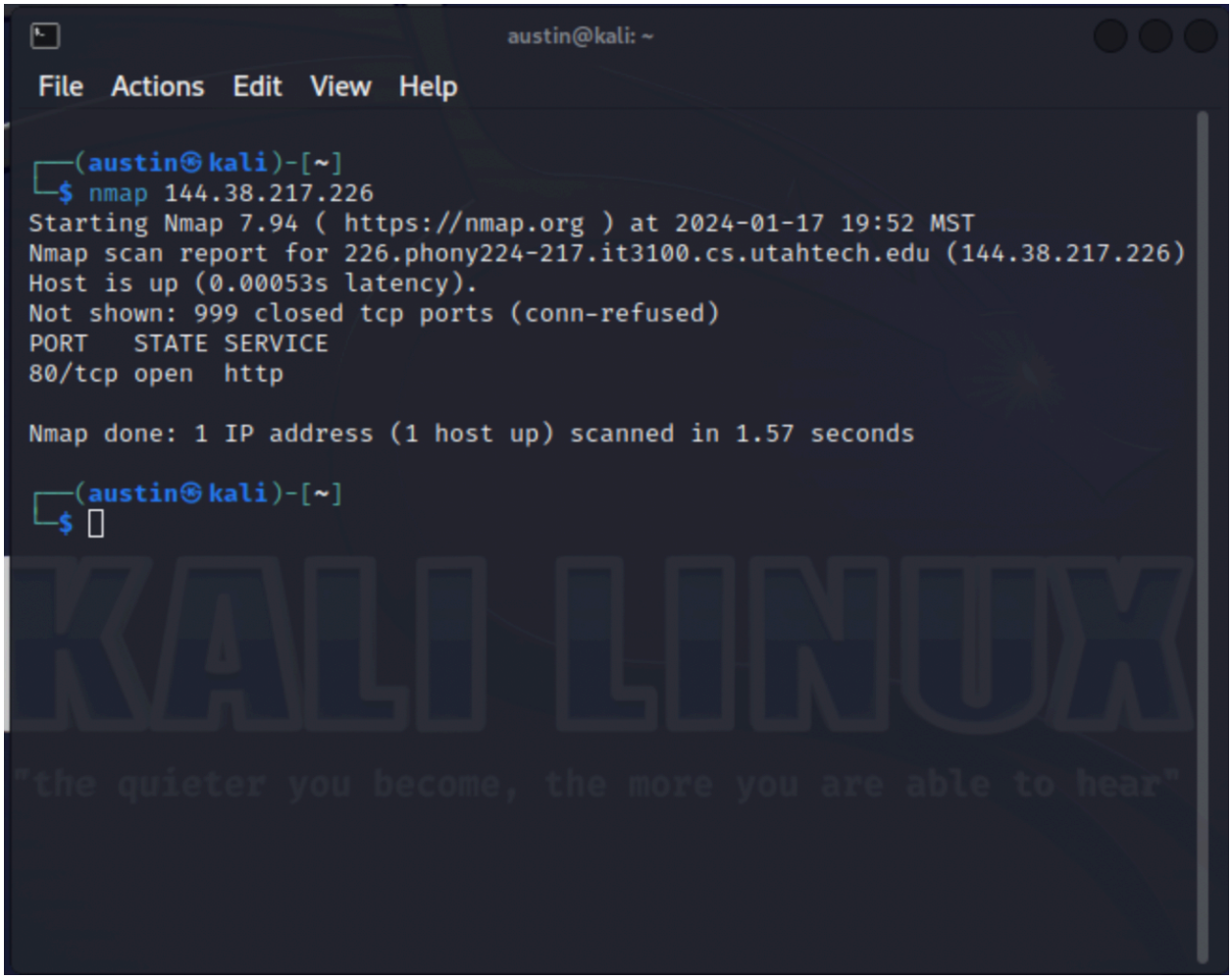
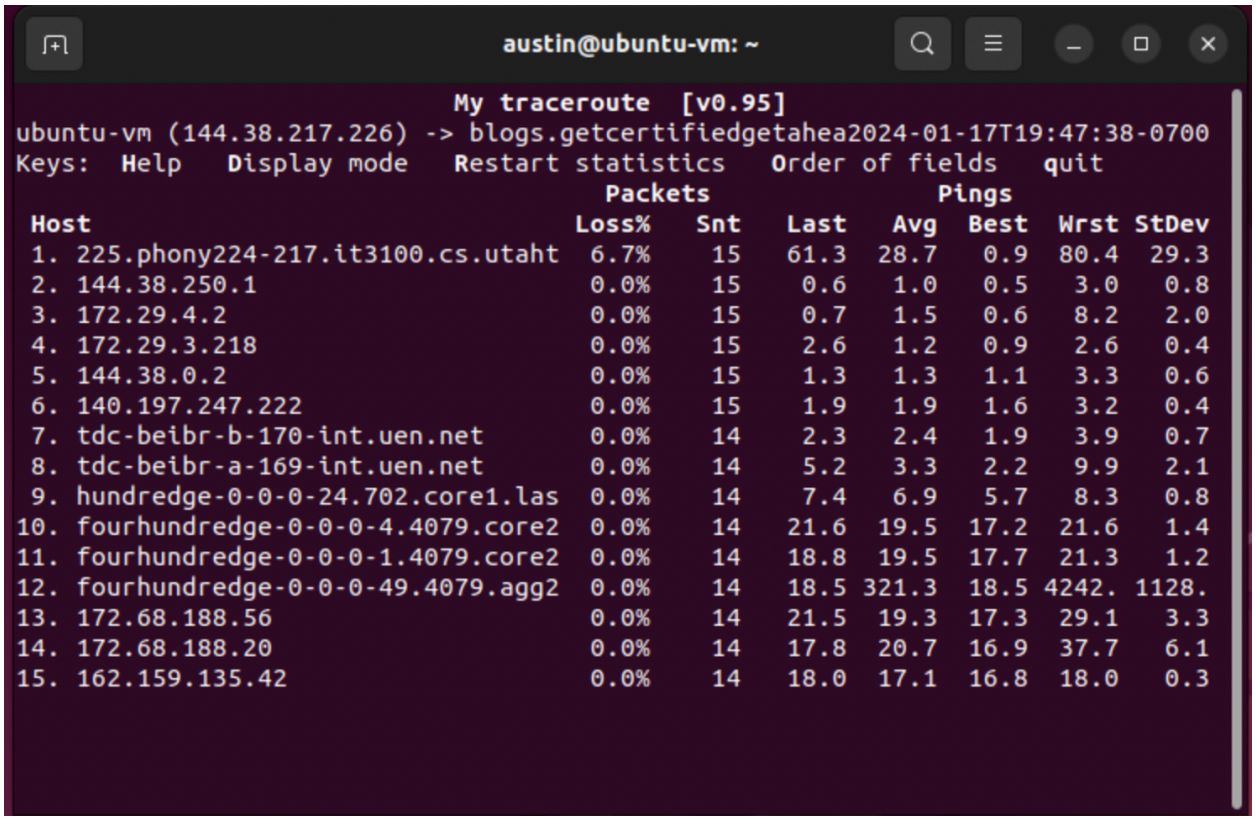

austin@ubuntu-vm: /var/log
Jan 17 19:49:47 ubuntu-vm systemd[1]: Reloading.
Jan 17 19:49:48 ubuntu-vm systemd[1]: message repeated 2 times: [Reloading.]
Jan 17 19:49:48 ubuntu-vm systemd[1]: Starting Daily apt download activities...
Jan 17 19:49:49 ubuntu-vm systemd[1]: apt-daily.service: Deactivated successfully.
Jan 17 19:49:49 ubuntu-vm systemd[1]: Finished Daily apt download activities.
austin@ubuntu-vm:/var/log$ logger
^C
austin@ubuntu-vm:/var/log$ logger "Log entry for Austin Davis, 1/17/2024 8:03pm"
austin@ubuntu-vm:/var/log$ tail syslog
Jan 17 19:49:46 ubuntu-vm systemd[1]: Reloading.
Jan 17 19:49:47 ubuntu-vm systemd[1]: Reloading.
Jan 17 19:49:47 ubuntu-vm systemd[1]: Starting Disk Cache Cleaning Daemon for Apache HTTP Server...
Jan 17 19:49:47 ubuntu-vm systemd[1]: Started Disk Cache Cleaning Daemon for Apache HTTP Server.
Jan 17 19:49:47 ubuntu-vm systemd[1]: Reloading.
Jan 17 19:49:48 ubuntu-vm systemd[1]: message repeated 2 times: [Reloading.]
Jan 17 19:49:48 ubuntu-vm systemd[1]: Starting Daily apt download activities...
Jan 17 19:49:49 ubuntu-vm systemd[1]: apt-daily.service: Deactivated successfully.
Jan 17 19:49:49 ubuntu-vm systemd[1]: Finished Daily apt download activities.
Jan 17 20:03:52 ubuntu-vm austin: Log entry for Austin Davis, 1/17/2024 8:03pm
austin@ubuntu-vm:/var/log$

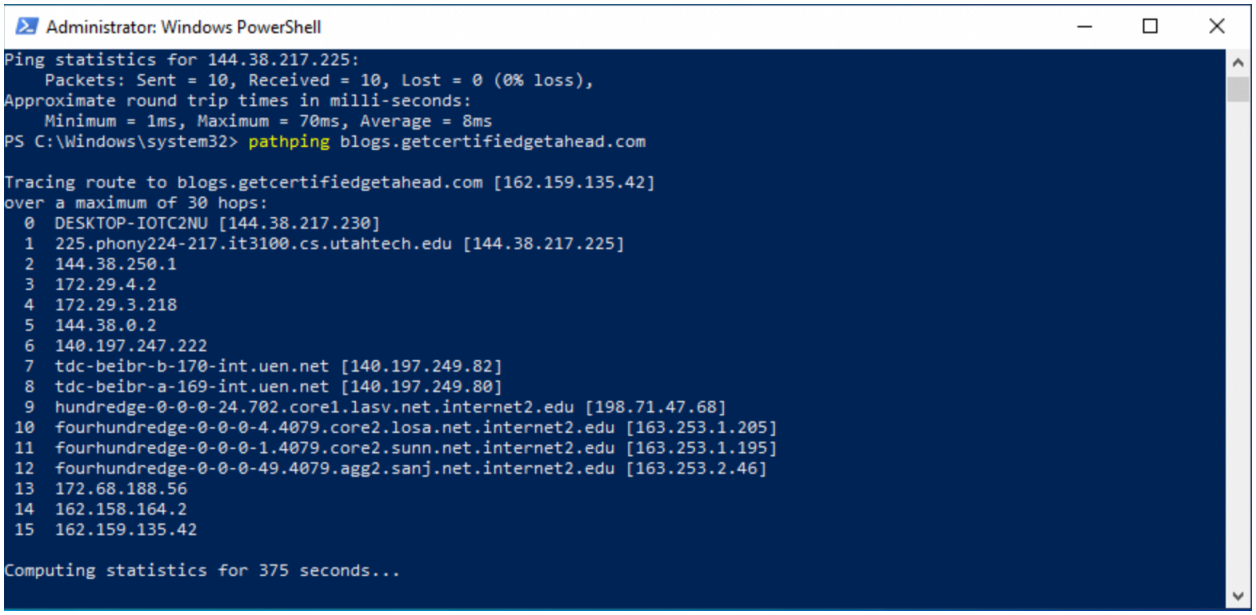

Event Properties - Event 1000, Application Error
General
Details
Friendly View
XML View
StartMenuExperienceHost.exe
0.0.0.0
5d65fb6a
Windows.UI.Xaml.dll
10.0.18362.449
b90db728
c000027b
0000000000712ec0
9f4
01da46f5505a2ab2
C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe
C:\Windows\System32\Windows.UI.Xaml.dll
e6c3ce0f-b876-4e2e-9dcb-a8556f2c9693
Microsoft.Windows.StartMenuExperienceHost_10.0.18362.449_neutral_neutral_cw5n1h2txyewy
App
Activate Windows
Go to Settings to activate Windows.
Copy
Close

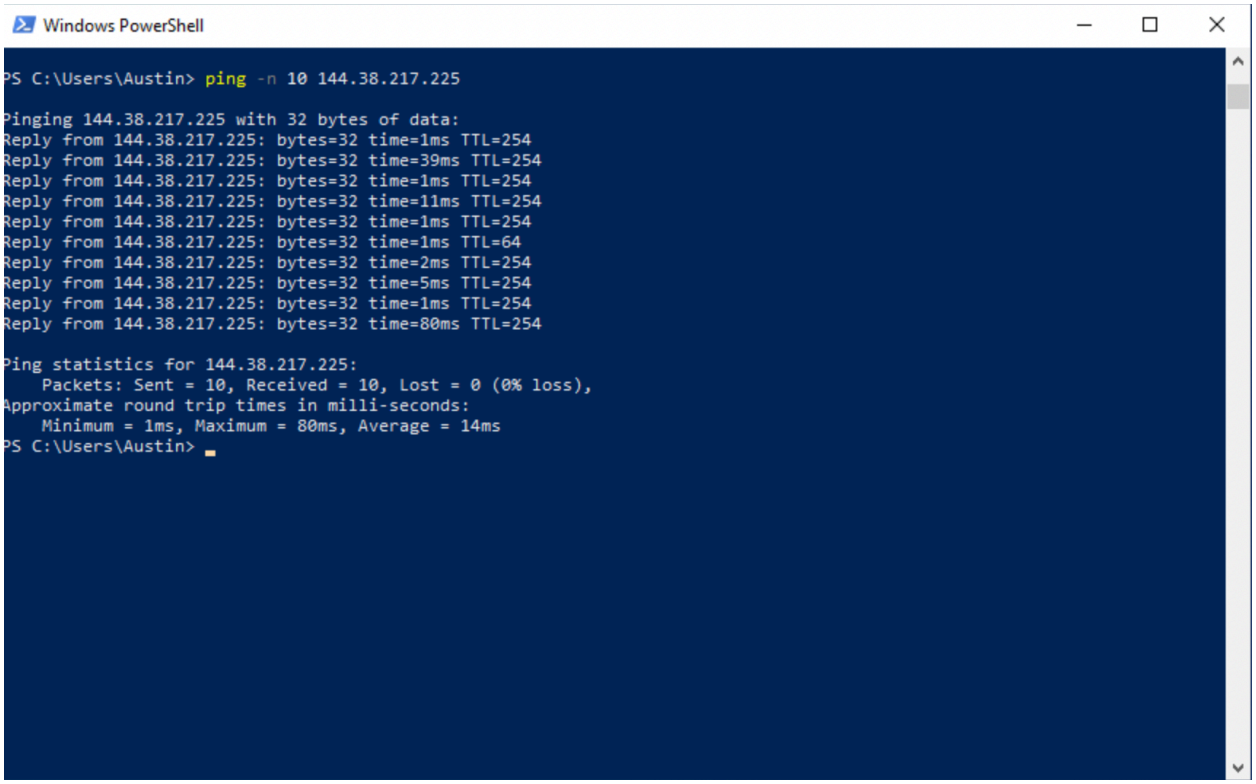

localhost:6085 (QEMU (d00436865-windows)) - RealVNC Viewer
Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Administrative Events
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Lo
Subscriptions
Security Number of events: 20,782
Filtered: Log: Security; Source: ; Event ID: 4624. Number of events: 398
Keywor... Date and Time Source Event ID Task Ca...
Audi... 1/18/2024 2:56:33 AM Micros... 4624 Logon
Audi... 1/18/2024 2:51:51 AM Micros... 4624 Logon
Audi... 1/18/2024 2:47:00 AM Micros... 4624 Logon
Audi... 1/18/2024 2:40:41 AM Micros... 4624 Logon
Audi... 1/17/2024 9:19:40 PM Micros... 4624 Logon
Audi... 1/17/2024 9:11:46 PM Micros... 4624 Logon
Audi... 1/17/2024 8:25:29 PM Micros... 4624 Logon
Audi... 1/17/2024 7:56:43 PM Micros... 4624 Logon
Audi... 1/17/2024 7:52:33 PM Micros... 4624 Logon
Audi... 1/17/2024 7:36:25 PM Micros... 4624 Logon
Audi... 1/17/2024 7:20:17 PM Micros... 4624 Logon
Audi... 1/17/2024 7:11:50 PM Micros... 4624 Logon
Audi... 1/17/2024 5:52:25 PM Micros... 4624 Logon
Audi... 1/17/2024 5:52:23 PM Micros... 4624 Logon
Audi... 1/17/2024 5:52:23 PM Micros... 4624 Logon
Audi... 1/17/2024 5:51:17 PM Micros... 4624 Logon
Event 4624, Microsoft Windows security auditing.
General Details
Friendly View XML View
SubjectUserSid S-1-5-18
SubjectUserName WIN-DRO5LB4BNSE$
SubjectDomainName WORKGROUP
SubjectLogonId 0x3e7
TargetUserSid S-1-5-18
Actions
Security
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Clear Filter
Properties
Find...
Save Filtered Log File A...
Attach a Task To this L...
Save Filter to Custom ...
View
Refresh
Help
Event 4624, Microsoft Wind...
Event Properties
Attach Task To This Eve...
Copy
Save Selected Events...
Refresh
Help
Activate Windows
Go to Settings to activate Windows.
Creates a filter.

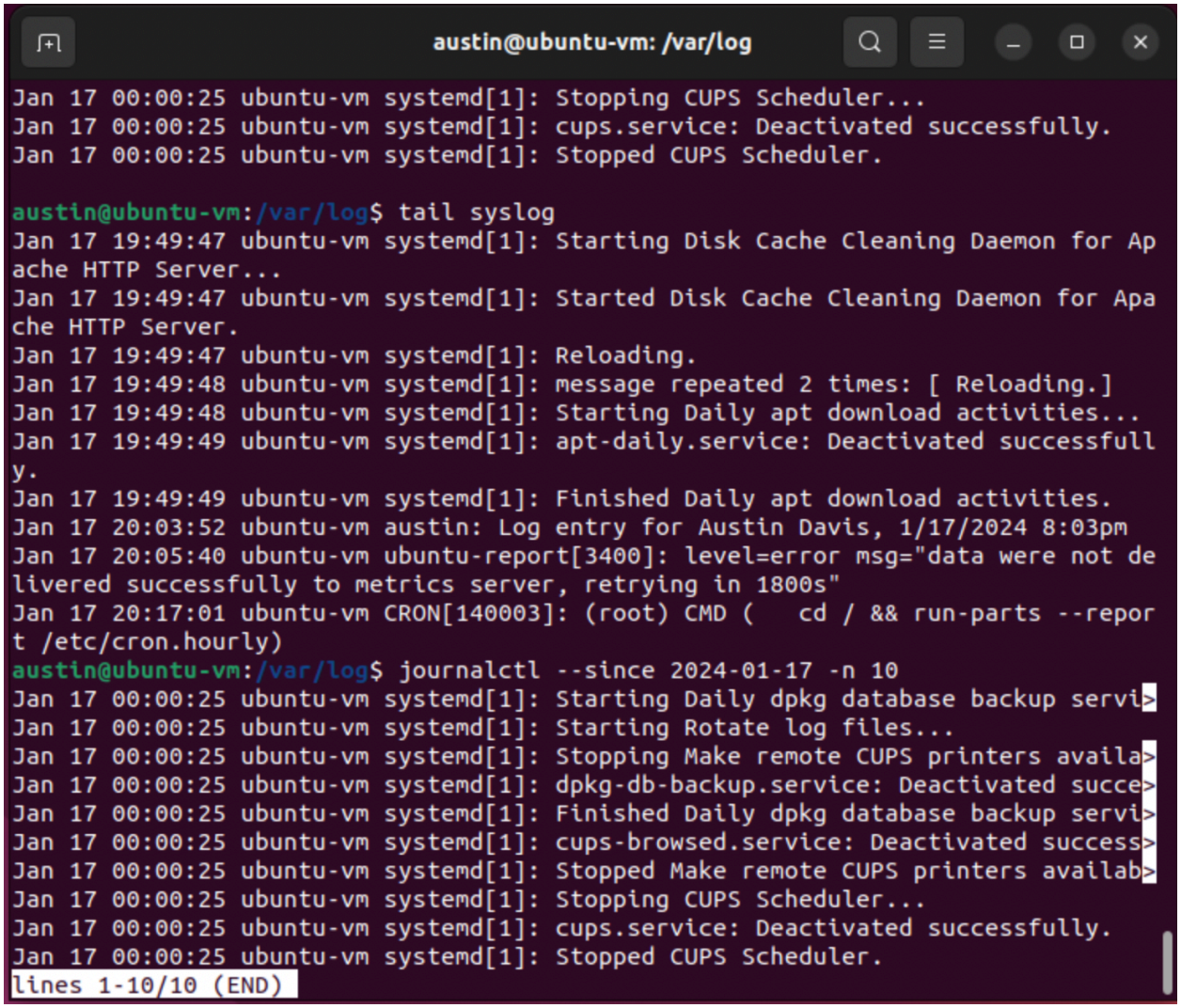

austin@kali: ~
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds
┌──(austin㉿kali)-[~]
└─$ sudo hping3 -S -p 80 144.38.217.226
[sudo] password for austin:
HPING 144.38.217.226 (eth0 144.38.217.226): S set, 40 headers + 0 data bytes
len=46 ip=144.38.217.226 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=64240 rtt
=7.6 ms
len=46 ip=144.38.217.226 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=64240 rtt
=6.8 ms
len=46 ip=144.38.217.226 ttl=64 DF id=0 sport=80 flags=SA seq=2 win=64240 rtt
=2.6 ms
len=46 ip=144.38.217.226 ttl=64 DF id=0 sport=80 flags=SA seq=3 win=64240 rtt
=2.3 ms
len=46 ip=144.38.217.226 ttl=64 DF id=0 sport=80 flags=SA seq=4 win=64240 rtt
=2.0 ms
len=46 ip=144.38.217.226 ttl=64 DF id=0 sport=80 flags=SA seq=6 win=64240 rtt
=1.4 ms
len=46 ip=144.38.217.226 ttl=64 DF id=0 sport=80 flags=SA seq=7 win=64240 rtt
=0.8 ms
len=46 ip=144.38.217.226 ttl=64 DF id=0 sport=80 flags=SA seq=8 win=64240 rtt
=8.5 ms
len=46 ip=144.38.217.226 ttl=64 DF id=0 sport=80 flags=SA seq=9 win=64240 rtt
=8.3 ms
len=46 ip=144.38.217.226 ttl=64 DF id=0 sport=80 flags=SA seq=10 win=64240 rt
t=8.0 ms
len=46 ip=144.38.217.226 ttl=64 DF id=0 sport=80 flags=SA seq=11 win=64240 rt


austin@kali: ~
File Actions Edit View Help
(austin㉿kali)-[~]
$ nmap 144.38.217.226
Starting Nmap 7.94 (https://nmap.org) at 2024-01-17 19:52 MST
Nmap scan report for 226.phony224-217.it3100.cs.utahtech.edu (144.38.217.226)
Host is up (0.00053s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT STATE SERVICE
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds
(austin㉿kali)-[~]
$
KALI LINUX
"the quieter you become, the more you are able to hear"


austin@ubuntu-vm: ~
My traceroute [v0.95]
ubuntu-vm (144.38.217.226) -> blogs.getcertifiedgetahea2024-01-17T19:47:38-0700
Keys: Help Display mode Restart statistics Order of fields quit
Packets Pings
Host Loss% Snt Last Avg Best Wrst StDev
1. 225.phony224-217.it3100.cs.utaht 6.7% 15 61.3 28.7 0.9 80.4 29.3
2. 144.38.250.1 0.0% 15 0.6 1.0 0.5 3.0 0.8
3. 172.29.4.2 0.0% 15 0.7 1.5 0.6 8.2 2.0
4. 172.29.3.218 0.0% 15 2.6 1.2 0.9 2.6 0.4
5. 144.38.0.2 0.0% 15 1.3 1.3 1.1 3.3 0.6
6. 140.197.247.222 0.0% 15 1.9 1.9 1.6 3.2 0.4
7. tdc-beibr-b-170-int.uen.net 0.0% 14 2.3 2.4 1.9 3.9 0.7
8. tdc-beibr-a-169-int.uen.net 0.0% 14 5.2 3.3 2.2 9.9 2.1
9. hundredge-0-0-0-24.702.core1.las 0.0% 14 7.4 6.9 5.7 8.3 0.8
10. fourhundredge-0-0-0-4.4079.core2 0.0% 14 21.6 19.5 17.2 21.6 1.4
11. fourhundredge-0-0-0-1.4079.core2 0.0% 14 18.8 19.5 17.7 21.3 1.2
12. fourhundredge-0-0-0-49.4079.agg2 0.0% 14 18.5 321.3 18.5 4242. 1128.
13. 172.68.188.56 0.0% 14 21.5 19.3 17.3 29.1 3.3
14. 172.68.188.20 0.0% 14 17.8 20.7 16.9 37.7 6.1
15. 162.159.135.42 0.0% 14 18.0 17.1 16.8 18.0 0.3


Administrator: Windows PowerShell
Ping statistics for 144.38.217.225:
Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 70ms, Average = 8ms
PS C:\Windows\system32> pathping blogs.getcertifiedgetahead.com
Tracing route to blogs.getcertifiedgetahead.com [162.159.135.42]
over a maximum of 30 hops:
0 DESKTOP-IOTC2NU [144.38.217.230]
1 225.phony224-217.it3100.cs.utahtech.edu [144.38.217.225]
2 144.38.250.1
3 172.29.4.2
4 172.29.3.218
5 144.38.0.2
6 140.197.247.222
7 tdc-beibr-b-170-int.uen.net [140.197.249.82]
8 tdc-beibr-a-169-int.uen.net [140.197.249.80]
9 hundredge-0-0-0-24.702.core1.lasv.net.internet2.edu [198.71.47.68]
10 fourhundredge-0-0-0-4.4079.core2.losa.net.internet2.edu [163.253.1.205]
11 fourhundredge-0-0-0-1.4079.core2.sunn.net.internet2.edu [163.253.1.195]
12 fourhundredge-0-0-0-49.4079.agg2.sanj.net.internet2.edu [163.253.2.46]
13 172.68.188.56
14 162.158.164.2
15 162.159.135.42
Computing statistics for 375 seconds...


Windows PowerShell
PS C:\Users\Austin> ping -n 10 144.38.217.225
Pinging 144.38.217.225 with 32 bytes of data:
Reply from 144.38.217.225: bytes=32 time=1ms TTL=254
Reply from 144.38.217.225: bytes=32 time=39ms TTL=254
Reply from 144.38.217.225: bytes=32 time=1ms TTL=254
Reply from 144.38.217.225: bytes=32 time=11ms TTL=254
Reply from 144.38.217.225: bytes=32 time=1ms TTL=254
Reply from 144.38.217.225: bytes=32 time=1ms TTL=64
Reply from 144.38.217.225: bytes=32 time=2ms TTL=254
Reply from 144.38.217.225: bytes=32 time=5ms TTL=254
Reply from 144.38.217.225: bytes=32 time=1ms TTL=254
Reply from 144.38.217.225: bytes=32 time=80ms TTL=254
Ping statistics for 144.38.217.225:
Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 80ms, Average = 14ms
PS C:\Users\Austin>


austin@ubuntu-vm: /var/log
Jan 17 00:00:25 ubuntu-vm systemd[1]: Stopping CUPS Scheduler...
Jan 17 00:00:25 ubuntu-vm systemd[1]: cups.service: Deactivated successfully.
Jan 17 00:00:25 ubuntu-vm systemd[1]: Stopped CUPS Scheduler.
austin@ubuntu-vm:/var/log$ tail syslog
Jan 17 19:49:47 ubuntu-vm systemd[1]: Starting Disk Cache Cleaning Daemon for Apache HTTP Server...
Jan 17 19:49:47 ubuntu-vm systemd[1]: Started Disk Cache Cleaning Daemon for Apache HTTP Server.
Jan 17 19:49:47 ubuntu-vm systemd[1]: Reloading.
Jan 17 19:49:48 ubuntu-vm systemd[1]: message repeated 2 times: [Reloading.]
Jan 17 19:49:48 ubuntu-vm systemd[1]: Starting Daily apt download activities...
Jan 17 19:49:49 ubuntu-vm systemd[1]: apt-daily.service: Deactivated successfully.
Jan 17 19:49:49 ubuntu-vm systemd[1]: Finished Daily apt download activities.
Jan 17 20:03:52 ubuntu-vm austin: Log entry for Austin Davis, 1/17/2024 8:03pm
Jan 17 20:05:40 ubuntu-vm ubuntu-report[3400]: level=error msg="data were not delivered successfully to metrics server, retrying in 1800s"
Jan 17 20:17:01 ubuntu-vm CRON[140003]: (root) CMD (cd / && run-parts --report /etc/cron.hourly)
austin@ubuntu-vm:/var/log$ journalctl --since 2024-01-17 -n 10
Jan 17 00:00:25 ubuntu-vm systemd[1]: Starting Daily dpkg database backup servi>
Jan 17 00:00:25 ubuntu-vm systemd[1]: Starting Rotate log files...
Jan 17 00:00:25 ubuntu-vm systemd[1]: Stopping Make remote CUPS printers availa>
Jan 17 00:00:25 ubuntu-vm systemd[1]: dpkg-db-backup.service: Deactivated succe>
Jan 17 00:00:25 ubuntu-vm systemd[1]: Finished Daily dpkg database backup servi>
Jan 17 00:00:25 ubuntu-vm systemd[1]: cups-browsed.service: Deactivated success>
Jan 17 00:00:25 ubuntu-vm systemd[1]: Stopped Make remote CUPS printers availab>
Jan 17 00:00:25 ubuntu-vm systemd[1]: Stopping CUPS Scheduler...
Jan 17 00:00:25 ubuntu-vm systemd[1]: cups.service: Deactivated successfully.
Jan 17 00:00:25 ubuntu-vm systemd[1]: Stopped CUPS Scheduler.
lines 1-10/10 (END)