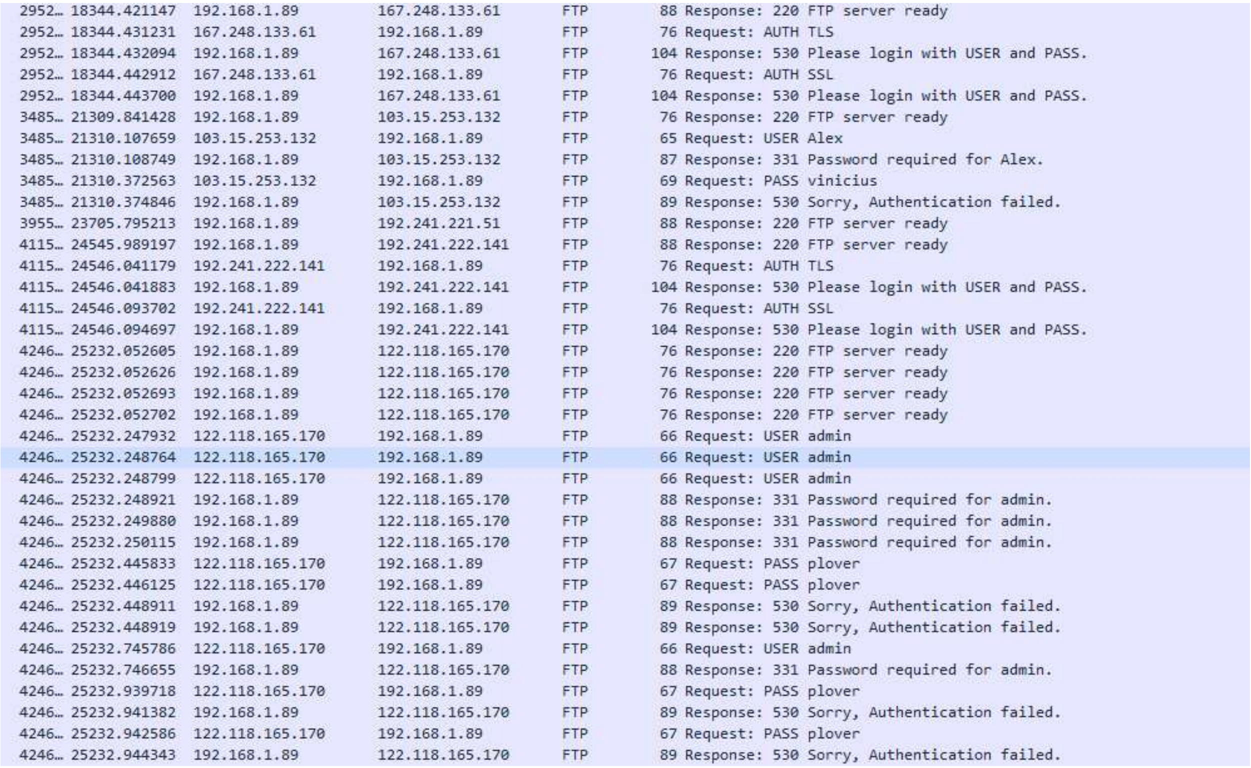
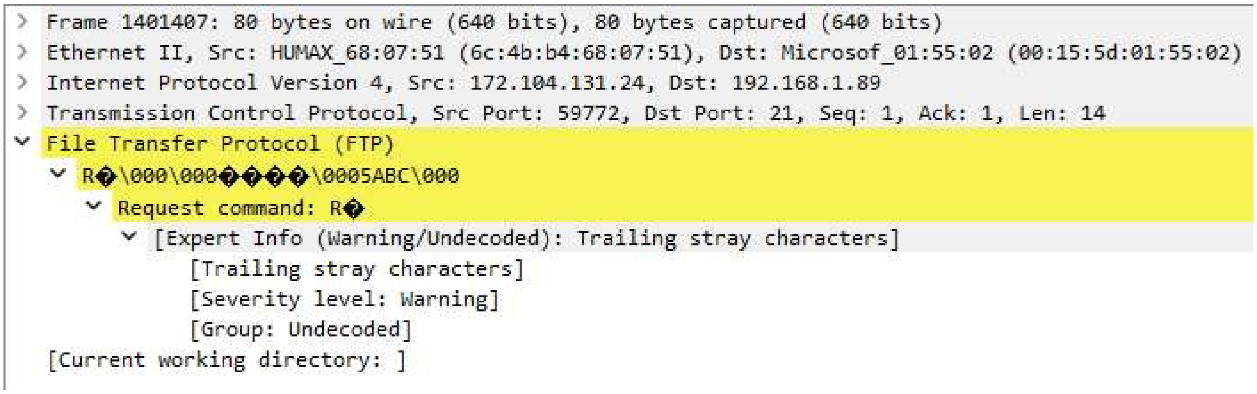
Timothy Reidy
9/8/2023
HA01



```
2952… 18344.421147  192.168.1.89     167.248.133.61   FTP    88 Response: 220 FTP server ready
2952… 18344.431231  167.248.133.61   192.168.1.89     FTP    76 Request: AUTH TLS
2952… 18344.432094  192.168.1.89     167.248.133.61   FTP   104 Response: 530 Please login with USER and PASS.
2952… 18344.442912  167.248.133.61   192.168.1.89     FTP    76 Request: AUTH SSL
2952… 18344.443700  192.168.1.89     167.248.133.61   FTP   104 Response: 530 Please login with USER and PASS.
3485… 21309.841428  192.168.1.89     103.15.253.132   FTP    76 Response: 220 FTP server ready
3485… 21310.107659  103.15.253.132   192.168.1.89     FTP    65 Request: USER Alex
3485… 21310.108749  192.168.1.89     103.15.253.132   FTP    87 Response: 331 Password required for Alex.
3485… 21310.372563  103.15.253.132   192.168.1.89     FTP    69 Request: PASS vinicius
3485… 21310.374846  192.168.1.89     103.15.253.132   FTP    89 Response: 530 Sorry, Authentication failed.
3955… 23705.795213  192.168.1.89     192.241.221.51   FTP    88 Response: 220 FTP server ready
4115… 24545.989197  192.168.1.89     192.241.222.141  FTP    88 Response: 220 FTP server ready
4115… 24546.041179  192.241.222.141  192.168.1.89     FTP    76 Request: AUTH TLS
4115… 24546.041883  192.168.1.89     192.241.222.141  FTP   104 Response: 530 Please login with USER and PASS.
4115… 24546.093702  192.241.222.141  192.168.1.89     FTP    76 Request: AUTH SSL
4115… 24546.094697  192.168.1.89     192.241.222.141  FTP   104 Response: 530 Please login with USER and PASS.
4246… 25232.052605  192.168.1.89     122.118.165.170  FTP    76 Response: 220 FTP server ready
4246… 25232.052626  192.168.1.89     122.118.165.170  FTP    76 Response: 220 FTP server ready
4246… 25232.052693  192.168.1.89     122.118.165.170  FTP    76 Response: 220 FTP server ready
4246… 25232.052702  192.168.1.89     122.118.165.170  FTP    76 Response: 220 FTP server ready
4246… 25232.247932  122.118.165.170  192.168.1.89     FTP    66 Request: USER admin
4246… 25232.248764  122.118.165.170  192.168.1.89     FTP    66 Request: USER admin
4246… 25232.248799  122.118.165.170  192.168.1.89     FTP    66 Request: USER admin
4246… 25232.248921  192.168.1.89     122.118.165.170  FTP    88 Response: 331 Password required for admin.
4246… 25232.249880  192.168.1.89     122.118.165.170  FTP    88 Response: 331 Password required for admin.
4246… 25232.250115  192.168.1.89     122.118.165.170  FTP    88 Response: 331 Password required for admin.
4246… 25232.445833  122.118.165.170  192.168.1.89     FTP    67 Request: PASS plover
4246… 25232.446125  122.118.165.170  192.168.1.89     FTP    67 Request: PASS plover
4246… 25232.448911  192.168.1.89     122.118.165.170  FTP    89 Response: 530 Sorry, Authentication failed.
4246… 25232.448919  192.168.1.89     122.118.165.170  FTP    89 Response: 530 Sorry, Authentication failed.
4246… 25232.745786  122.118.165.170  192.168.1.89     FTP    66 Request: USER admin
4246… 25232.746655  192.168.1.89     122.118.165.170  FTP    88 Response: 331 Password required for admin.
4246… 25232.939718  122.118.165.170  192.168.1.89     FTP    67 Request: PASS plover
4246… 25232.941382  192.168.1.89     122.118.165.170  FTP    89 Response: 530 Sorry, Authentication failed.
4246… 25232.942586  122.118.165.170  192.168.1.89     FTP    67 Request: PASS plover
4246… 25232.944343  192.168.1.89     122.118.165.170  FTP    89 Response: 530 Sorry, Authentication failed.
```

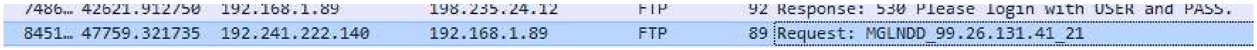
I was not able to capture it all in one screenshot, but the capture of FTP traffic was rather interesting. It looks like the IP 122.118.165.170 was attempting to authenticate themselves as an admin, but was failing to authenticate. Based on the repeated use of the incorrect password, I would assume it is not malicious and instead an admin with an incorrect password, but it would be worth looking into. Additionally, there was an interesting packet that I have screenshotted below.f



```
> Frame 1401407: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)
> Ethernet II, Src: HUMAX_68:07:51 (6c:4b:b4:68:07:51), Dst: Microsof_01:55:02 (00:15:5d:01:55:02)
> Internet Protocol Version 4, Src: 172.104.131.24, Dst: 192.168.1.89
> Transmission Control Protocol, Src Port: 59772, Dst Port: 21, Seq: 1, Ack: 1, Len: 14
v File Transfer Protocol (FTP)
  v R�\000\000����\0005ABC\000
    v Request command: R�
      v [Expert Info (Warning/Undecoded): Trailing stray characters]
          [Trailing stray characters]
          [Severity level: Warning]
          [Group: Undecoded]
  [Current working directory: ]
```

I poked around but couldn’t find any specific reason for this that I know of. I can only guess that it has something to do with attempting to bypass authentication. They additionally tried to login as a guest user with a fake email, but this login was rejected as well.

One more interesting looking packet is below.

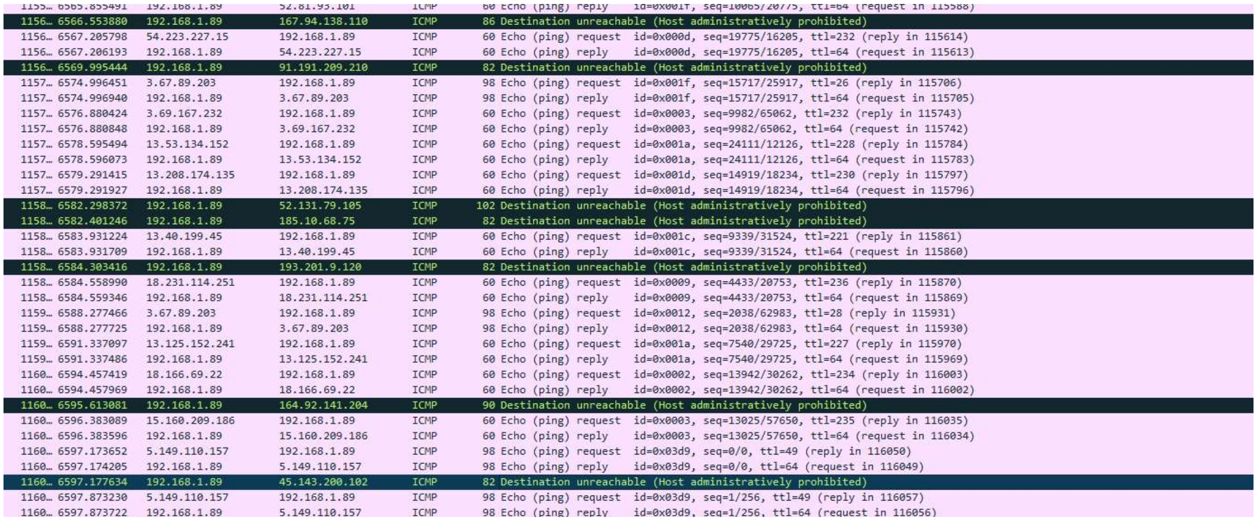


```
7486… 42621.912750  192.168.1.89       198.235.24.12     FTP        92 Response: 530 Please login with USER and PASS.
8451… 47759.321735  192.241.222.140    192.168.1.89      FTP        89 Request: MGLNDD_99.26.131.41_21
```

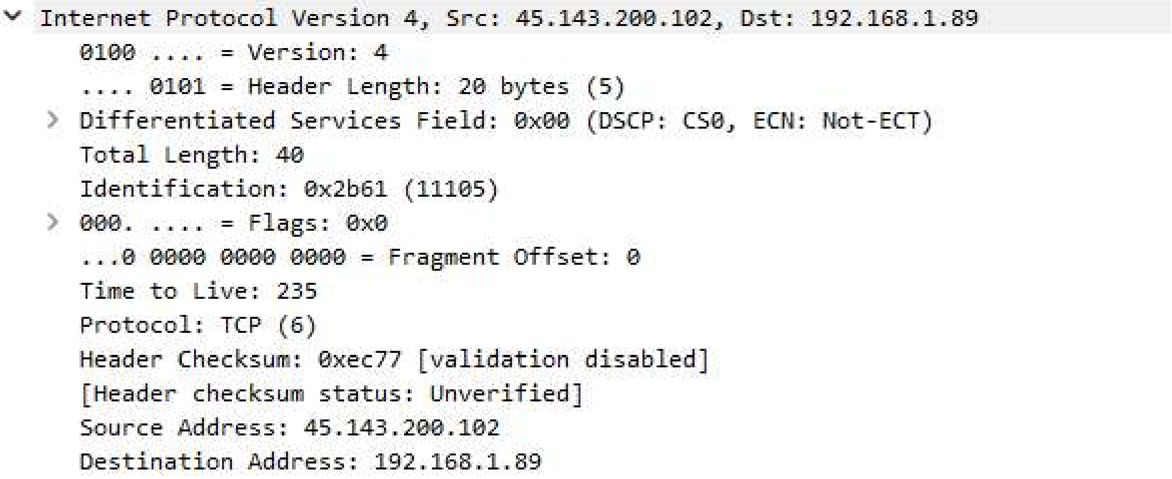
This activity is not malicious but it appeared to me as weird initially. It is from a company that does scans of networks to help identify organizations' online services. They scan a ton, and often their traffic is a nuisance to people looking at logs.

I looked through the SSH and SNMP, but nothing caught my eye when I was browsing those packets.

As for ICMP, I did see some interesting packets in that list.



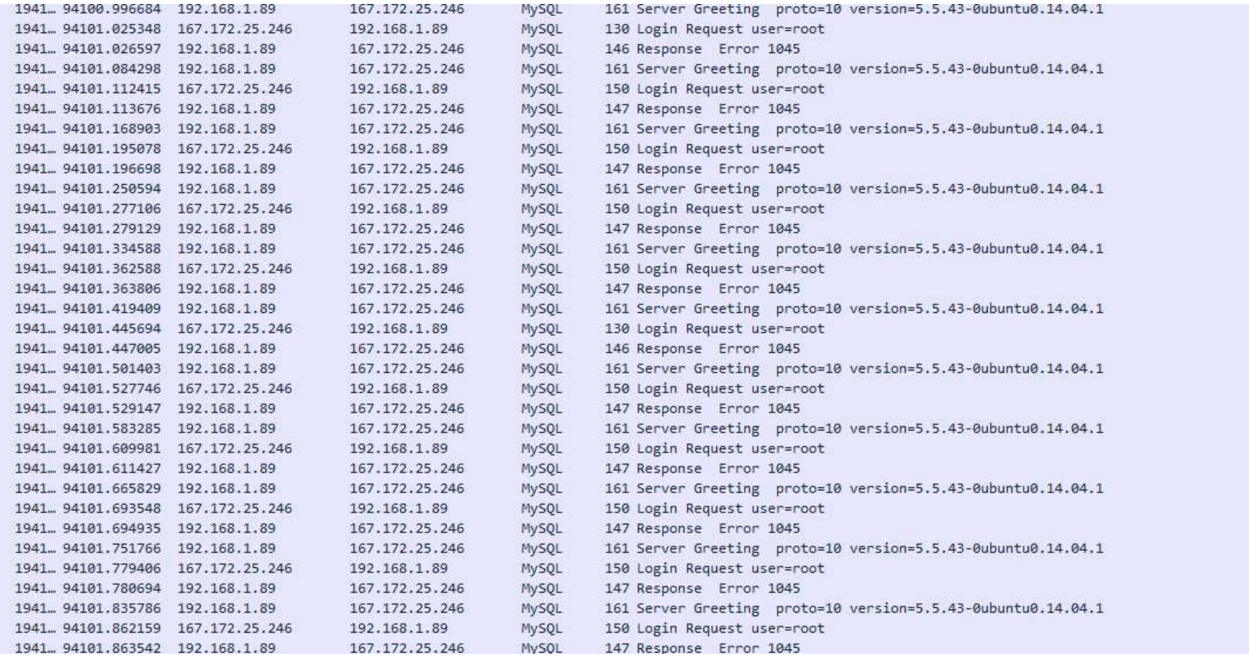
```
1155… 6565.855491  192.168.1.89     52.81.93.101     ICMP   60 Echo (ping) reply    id=0x001f, seq=10065/20775, ttl=64 (request in 115588)
1156… 6566.553880  192.168.1.89     167.94.138.110   ICMP   86 Destination unreachable (Host administratively prohibited)
1156… 6567.205798  54.223.227.15    192.168.1.89     ICMP   60 Echo (ping) request  id=0x000d, seq=19775/16205, ttl=232 (reply in 115614)
1156… 6567.206193  192.168.1.89     54.223.227.15    ICMP   60 Echo (ping) reply    id=0x000d, seq=19775/16205, ttl=64 (request in 115613)
1156… 6569.995444  192.168.1.89     91.191.209.210   ICMP   82 Destination unreachable (Host administratively prohibited)
1157… 6574.996451  3.67.89.203      192.168.1.89     ICMP   98 Echo (ping) request  id=0x001f, seq=15717/25917, ttl=26 (reply in 115706)
1157… 6574.996940  192.168.1.89     3.67.89.203      ICMP   98 Echo (ping) reply    id=0x001f, seq=15717/25917, ttl=64 (request in 115705)
1157… 6576.880424  3.69.167.232     192.168.1.89     ICMP   60 Echo (ping) request  id=0x0003, seq=9982/65062, ttl=232 (reply in 115743)
1157… 6576.880848  192.168.1.89     3.69.167.232     ICMP   60 Echo (ping) reply    id=0x0003, seq=9982/65062, ttl=64 (request in 115742)
1157… 6578.595494  13.53.134.152    192.168.1.89     ICMP   60 Echo (ping) request  id=0x001a, seq=24111/12126, ttl=228 (reply in 115784)
1157… 6578.596073  192.168.1.89     13.53.134.152    ICMP   60 Echo (ping) reply    id=0x001a, seq=24111/12126, ttl=64 (request in 115783)
1157… 6579.291415  13.208.174.135   192.168.1.89     ICMP   60 Echo (ping) request  id=0x001d, seq=14919/18234, ttl=230 (reply in 115797)
1157… 6579.291927  192.168.1.89     13.208.174.135   ICMP   60 Echo (ping) reply    id=0x001d, seq=14919/18234, ttl=64 (request in 115796)
1158… 6582.298372  192.168.1.89     52.131.79.105    ICMP  102 Destination unreachable (Host administratively prohibited)
1158… 6582.401246  192.168.1.89     185.10.68.75     ICMP   82 Destination unreachable (Host administratively prohibited)
1158… 6583.931224  13.40.199.45     192.168.1.89     ICMP   60 Echo (ping) request  id=0x001c, seq=9339/31524, ttl=221 (reply in 115861)
1158… 6583.931709  192.168.1.89     13.40.199.45     ICMP   60 Echo (ping) reply    id=0x001c, seq=9339/31524, ttl=64 (request in 115860)
1158… 6584.303416  192.168.1.89     193.201.9.120    ICMP   82 Destination unreachable (Host administratively prohibited)
1158… 6584.558990  18.231.114.251   192.168.1.89     ICMP   60 Echo (ping) request  id=0x0009, seq=4433/20753, ttl=236 (reply in 115870)
1158… 6584.559346  192.168.1.89     18.231.114.251   ICMP   60 Echo (ping) reply    id=0x0009, seq=4433/20753, ttl=64 (request in 115869)
1159… 6588.277466  3.67.89.203      192.168.1.89     ICMP   98 Echo (ping) request  id=0x0012, seq=2038/62983, ttl=28 (reply in 115931)
1159… 6588.277725  192.168.1.89     3.67.89.203      ICMP   98 Echo (ping) reply    id=0x0012, seq=2038/62983, ttl=64 (request in 115930)
1159… 6591.337097  13.125.152.241   192.168.1.89     ICMP   60 Echo (ping) request  id=0x001a, seq=7540/29725, ttl=227 (reply in 115970)
1159… 6591.337486  192.168.1.89     13.125.152.241   ICMP   60 Echo (ping) reply    id=0x001a, seq=7540/29725, ttl=64 (request in 115969)
1160… 6594.457419  18.166.69.22     192.168.1.89     ICMP   60 Echo (ping) request  id=0x0002, seq=13942/30262, ttl=234 (reply in 116003)
1160… 6594.457969  192.168.1.89     18.166.69.22     ICMP   60 Echo (ping) reply    id=0x0002, seq=13942/30262, ttl=64 (request in 116002)
1160… 6595.613081  192.168.1.89     164.92.141.204   ICMP   90 Destination unreachable (Host administratively prohibited)
1160… 6596.383089  15.160.209.186   192.168.1.89     ICMP   60 Echo (ping) request  id=0x0003, seq=13025/57650, ttl=235 (reply in 116035)
1160… 6596.383596  192.168.1.89     15.160.209.186   ICMP   60 Echo (ping) reply    id=0x0003, seq=13025/57650, ttl=64 (request in 116034)
1160… 6597.173652  5.149.110.157    192.168.1.89     ICMP   98 Echo (ping) request  id=0x03d9, seq=0/0, ttl=49 (reply in 116050)
1160… 6597.174205  192.168.1.89     5.149.110.157    ICMP   98 Echo (ping) reply    id=0x03d9, seq=0/0, ttl=64 (request in 116049)
1160… 6597.177634  192.168.1.89     45.143.200.102   ICMP   82 Destination unreachable (Host administratively prohibited)
1160… 6597.873230  5.149.110.157    192.168.1.89     ICMP   98 Echo (ping) request  id=0x03d9, seq=1/256, ttl=49 (reply in 116057)
1160… 6597.873722  192.168.1.89     5.149.110.157    ICMP   98 Echo (ping) reply    id=0x03d9, seq=1/256, ttl=64 (request in 116056)
```



```
⌄ Internet Protocol Version 4, Src: 45.143.200.102, Dst: 192.168.1.89
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 40
     Identification: 0x2b61 (11105)
   > 000. .... = Flags: 0x0
     ...0 0000 0000 0000 = Fragment Offset: 0
     Time to Live: 235
     Protocol: TCP (6)
     Header Checksum: 0xec77 [validation disabled]
     [Header checksum status: Unverified]
     Source Address: 45.143.200.102
     Destination Address: 192.168.1.89
```

I was especially checking the destination address. There are a ton of ICMP messages that are aimed at a destination of 192.168.1.89, which I would assume to be a server address, as that same IP sends some “Destination Unreachable because of host permissions” messages. This may be due to routine scanning or something not nefarious, but it is interesting to notice.

One last collection of interesting packets



```
1941… 94100.996684  192.168.1.89     167.172.25.246    MySQL    161 Server Greeting  proto=10 version=5.5.43-0ubuntu0.14.04.1
1941… 94101.025348  167.172.25.246   192.168.1.89      MySQL    130 Login Request user=root
1941… 94101.026597  192.168.1.89     167.172.25.246    MySQL    146 Response  Error 1045
1941… 94101.084298  192.168.1.89     167.172.25.246    MySQL    161 Server Greeting  proto=10 version=5.5.43-0ubuntu0.14.04.1
1941… 94101.112415  167.172.25.246   192.168.1.89      MySQL    150 Login Request user=root
1941… 94101.113676  192.168.1.89     167.172.25.246    MySQL    147 Response  Error 1045
1941… 94101.168903  192.168.1.89     167.172.25.246    MySQL    161 Server Greeting  proto=10 version=5.5.43-0ubuntu0.14.04.1
1941… 94101.195078  167.172.25.246   192.168.1.89      MySQL    150 Login Request user=root
1941… 94101.196698  192.168.1.89     167.172.25.246    MySQL    147 Response  Error 1045
1941… 94101.250594  192.168.1.89     167.172.25.246    MySQL    161 Server Greeting  proto=10 version=5.5.43-0ubuntu0.14.04.1
1941… 94101.277106  167.172.25.246   192.168.1.89      MySQL    150 Login Request user=root
1941… 94101.279129  192.168.1.89     167.172.25.246    MySQL    147 Response  Error 1045
1941… 94101.334588  192.168.1.89     167.172.25.246    MySQL    161 Server Greeting  proto=10 version=5.5.43-0ubuntu0.14.04.1
1941… 94101.362588  167.172.25.246   192.168.1.89      MySQL    150 Login Request user=root
1941… 94101.363806  192.168.1.89     167.172.25.246    MySQL    147 Response  Error 1045
1941… 94101.419409  192.168.1.89     167.172.25.246    MySQL    161 Server Greeting  proto=10 version=5.5.43-0ubuntu0.14.04.1
1941… 94101.445694  167.172.25.246   192.168.1.89      MySQL    130 Login Request user=root
1941… 94101.447005  192.168.1.89     167.172.25.246    MySQL    146 Response  Error 1045
1941… 94101.501403  192.168.1.89     167.172.25.246    MySQL    161 Server Greeting  proto=10 version=5.5.43-0ubuntu0.14.04.1
1941… 94101.527746  167.172.25.246   192.168.1.89      MySQL    150 Login Request user=root
1941… 94101.529147  192.168.1.89     167.172.25.246    MySQL    147 Response  Error 1045
1941… 94101.583285  192.168.1.89     167.172.25.246    MySQL    161 Server Greeting  proto=10 version=5.5.43-0ubuntu0.14.04.1
1941… 94101.609981  167.172.25.246   192.168.1.89      MySQL    150 Login Request user=root
1941… 94101.611427  192.168.1.89     167.172.25.246    MySQL    147 Response  Error 1045
1941… 94101.665829  192.168.1.89     167.172.25.246    MySQL    161 Server Greeting  proto=10 version=5.5.43-0ubuntu0.14.04.1
1941… 94101.693548  167.172.25.246   192.168.1.89      MySQL    150 Login Request user=root
1941… 94101.694935  192.168.1.89     167.172.25.246    MySQL    147 Response  Error 1045
1941… 94101.751766  192.168.1.89     167.172.25.246    MySQL    161 Server Greeting  proto=10 version=5.5.43-0ubuntu0.14.04.1
1941… 94101.779406  167.172.25.246   192.168.1.89      MySQL    150 Login Request user=root
1941… 94101.780694  192.168.1.89     167.172.25.246    MySQL    147 Response  Error 1045
1941… 94101.835786  192.168.1.89     167.172.25.246    MySQL    161 Server Greeting  proto=10 version=5.5.43-0ubuntu0.14.04.1
1941… 94101.862159  167.172.25.246   192.168.1.89      MySQL    150 Login Request user=root
1941… 94101.863542  192.168.1.89     167.172.25.246    MySQL    147 Response  Error 1045
```

This relates to the other probes for admin access, but this time it appears that the IP 167.172.25.246 is attempting to login with root. However when looking at multiple requests, and zooming into the MySQL protocol frame data, we can see that this IP was attempting many different passwords. The passwords are encrypted but it can be deciphered that they are different. Either this or possibly the same password hashed with different keys each time.

Deductions: I did not see anything that would be a gigantic security risk, but there were many many attempts to access root or admin roles, which is something that is worrying. Making sure that these roles are protected against these primitive probes is worth looking into, as well as defending against any more sophisticated attacks.

Skills Discussion: I have previously used wireshark before, but never on packets that are presumably somewhat malicious, which was quite interesting. I think most importantly I just solidified what each of the more prevalent protocols are, and what they are used for. I previously was not too sure of ICMP, or SMNP, or FTP, and was forced to really get them to examine the packets. Lastly, I enjoyed examining a packet capture with so many different types of protocols, as when I capture my own traffic I don’t get many of the more niche protocols displayed here.