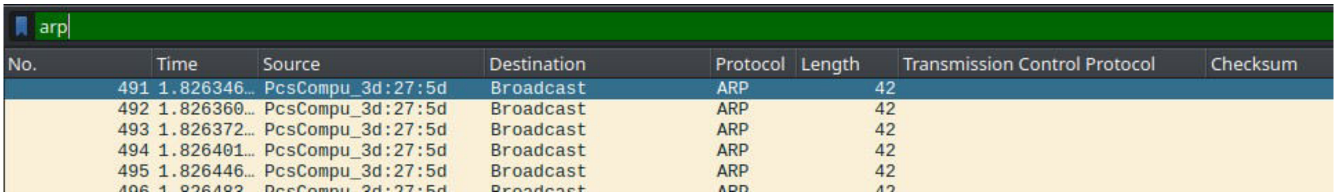
Network Analysis Challenge [Activity]

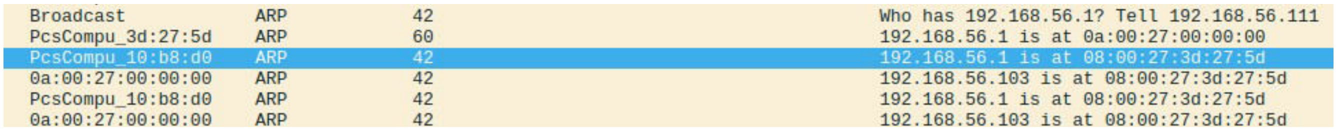
PCAP 3

1.What is the MAC address of the attacker?

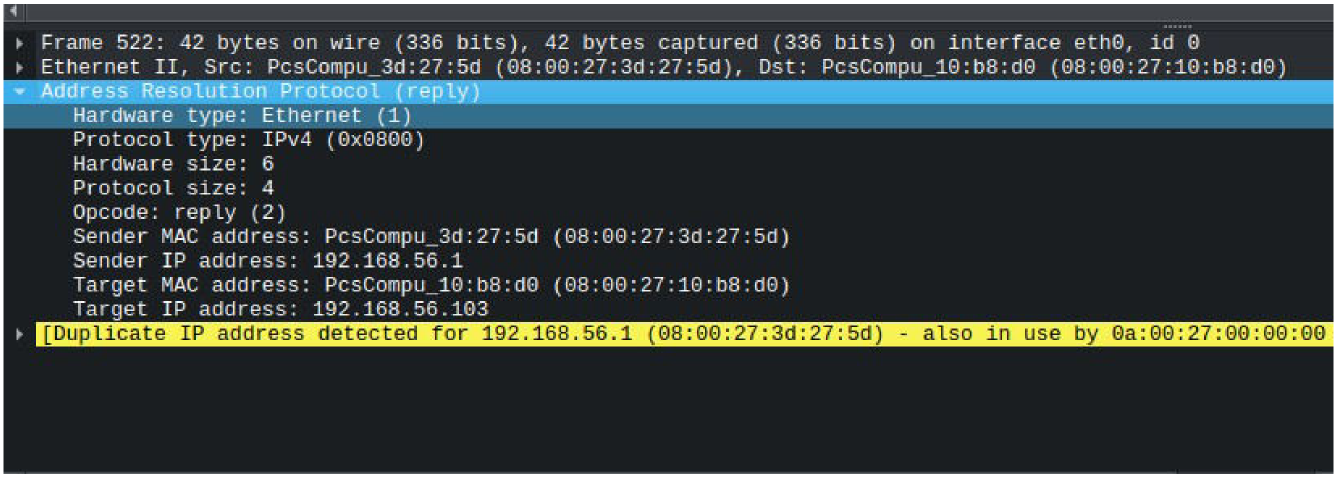
The attacker gained access through an used port into network. Need look into the 2nd layer of the OSI model. This can be a case of ARP poisoning attack. So search arp in the in display filter. Now ignore the destination as broadcast and go through all other packet to check if for a single IP address there is two mac addressed mapped. Follow these steps we will find the for the IP address 192.168.56.1 there will be two mac addressed mapped. The second mac address will be attacker's MAC address.



```
arp
No.          Time        Source             Destination        Protocol Length  Transmission Control Protocol  Checksum
         491 1.826346… PcsCompu_3d:27:5d  Broadcast          ARP          42
         492 1.826360… PcsCompu_3d:27:5d  Broadcast          ARP          42
         493 1.826372… PcsCompu_3d:27:5d  Broadcast          ARP          42
         494 1.826401… PcsCompu_3d:27:5d  Broadcast          ARP          42
         495 1.826446… PcsCompu_3d:27:5d  Broadcast          ARP          42
         496 1.826483… PcsCompu_3d:27:5d  Broadcast          ARP          42
```



```
Broadcast           ARP         42                          Who has 192.168.56.1? Tell 192.168.56.111
PcsCompu_3d:27:5d   ARP         60                          192.168.56.1 is at 0a:00:27:00:00:00
PcsCompu_10:b8:d0   ARP         42                          192.168.56.1 is at 08:00:27:3d:27:5d
0a:00:27:00:00:00   ARP         42                          192.168.56.103 is at 08:00:27:3d:27:5d
PcsCompu_10:b8:d0   ARP         42                          192.168.56.1 is at 08:00:27:3d:27:5d
0a:00:27:00:00:00   ARP         42                          192.168.56.103 is at 08:00:27:3d:27:5d
```



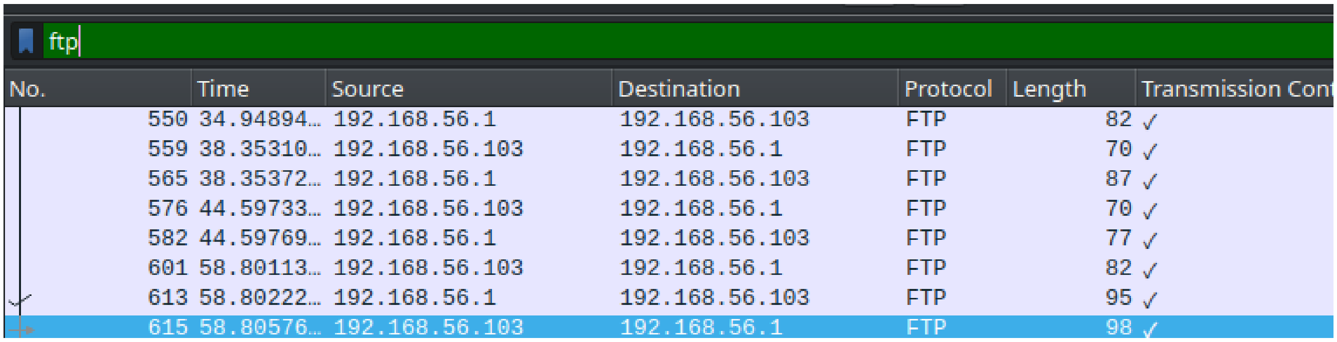
```
▸ Frame 522: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
▸ Ethernet II, Src: PcsCompu_3d:27:5d (08:00:27:3d:27:5d), Dst: PcsCompu_10:b8:d0 (08:00:27:10:b8:d0)
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: PcsCompu_3d:27:5d (08:00:27:3d:27:5d)
    Sender IP address: 192.168.56.1
    Target MAC address: PcsCompu_10:b8:d0 (08:00:27:10:b8:d0)
    Target IP address: 192.168.56.103
▸ [Duplicate IP address detected for 192.168.56.1 (08:00:27:3d:27:5d) - also in use by 0a:00:27:00:00:00
```

2. What is the type of attack which is taking place that allows the attacker to listen in on conversations between the central server and another host?

Man-in-the-Middle

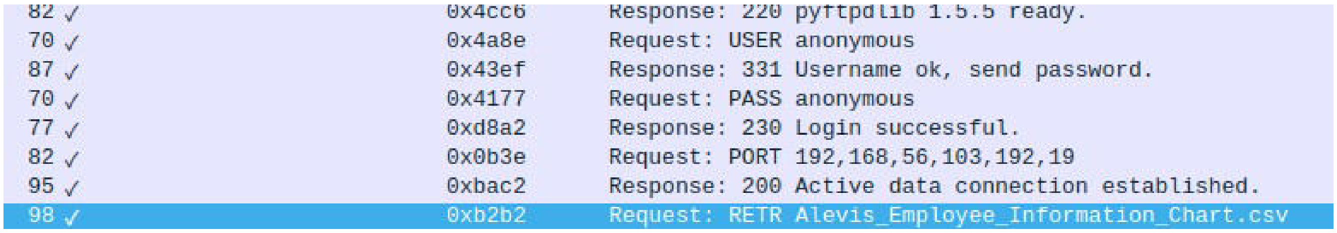
3.What is the file which was downloaded from the central server?

Search ‘ftp’ in the display filter. Check out through the info column of all the packet. See RETR request sent, it will ask the the server to send the contents of a file over the data connection already established by the client. The name of the file is Alevis_Employee_Information_Chart.csv.



ftp

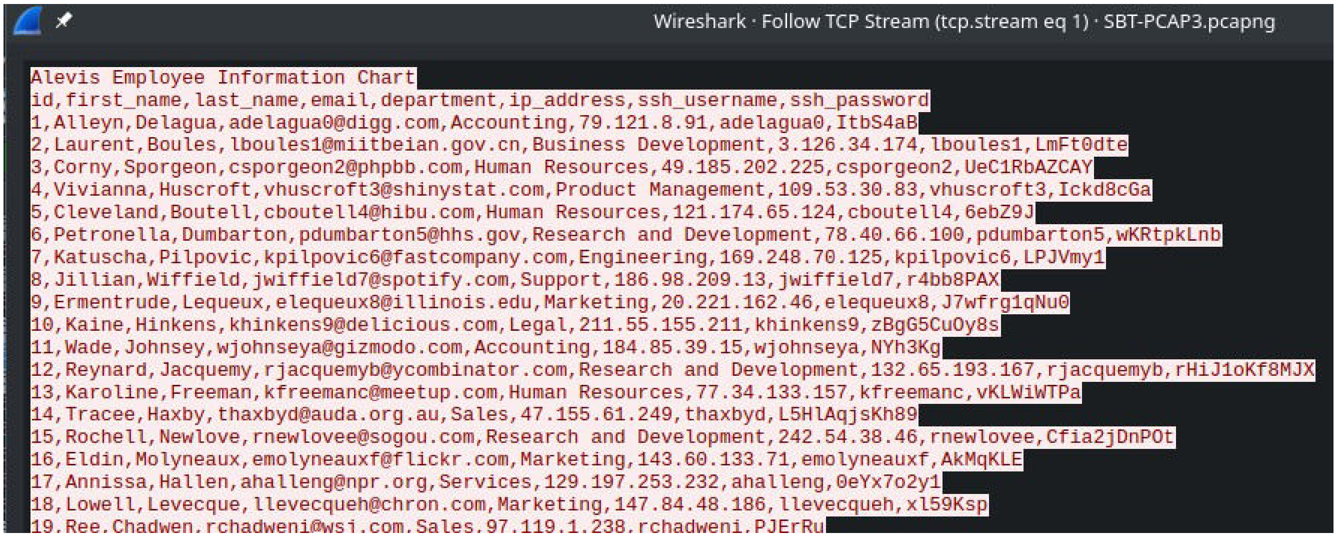
No.	Time	Source	Destination	Protocol	Length	Transmission Cont
550	34.94894…	192.168.56.1	192.168.56.103	FTP	82	✓
559	38.35310…	192.168.56.103	192.168.56.1	FTP	70	✓
565	38.35372…	192.168.56.1	192.168.56.103	FTP	87	✓
576	44.59733…	192.168.56.103	192.168.56.1	FTP	70	✓
582	44.59769…	192.168.56.1	192.168.56.103	FTP	77	✓
601	58.80113…	192.168.56.103	192.168.56.1	FTP	82	✓
613	58.80222…	192.168.56.1	192.168.56.103	FTP	95	✓
615	58.80576…	192.168.56.103	192.168.56.1	FTP	98	✓



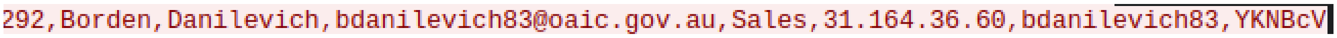
82 ✓	0x4cc6	Response: 220 pyftpdlib 1.5.5 ready.
70 ✓	0x4a8e	Request: USER anonymous
87 ✓	0x43ef	Response: 331 Username ok, send password.
70 ✓	0x4177	Request: PASS anonymous
77 ✓	0xd8a2	Response: 230 Login successful.
82 ✓	0x0b3e	Request: PORT 192,168,56,103,192,19
95 ✓	0xbac2	Response: 200 Active data connection established.
98 ✓	0xb2b2	Request: RETR Alevis_Employee_Information_Chart.csv

4.What department does Borden Danilevich work in?

Need to see in the Alevis_Employee_Information_Chart.csv. file to solve this and next question. To access the .csv file select the packet where we found the Alevis_Employee_Information_Chart.csv was found and choose follow and tcp stream for that packet and increase the stream to 1 in the bottom right corner of the new pop-up window. From the Alevis_Employee_Information_Chart.csv file we can find that Borden Danilevich works in the Sales department.


Wireshark · Follow TCP Stream (tcp.stream eq 1) · SBT-PCAP3.pcapng

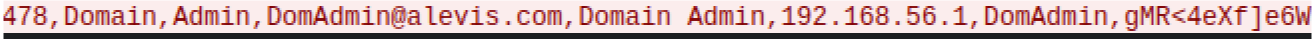
```
Alevis Employee Information Chart
id,first_name,last_name,email,department,ip_address,ssh_username,ssh_password
1,Alleyn,Delagua,adelagua0@digg.com,Accounting,79.121.8.91,adelagua0,ItbS4aB
2,Laurent,Boules,lboules1@miitbeian.gov.cn,Business Development,3.126.34.174,lboules1,LmFt0dte
3,Corny,Sporgeon,csporgeon2@phpbb.com,Human Resources,49.185.202.225,csporgeon2,UeC1RbAZCAY
4,Vivianna,Huscroft,vhuscroft3@shinystat.com,Product Management,109.53.30.83,vhuscroft3,Ickd8cGa
5,Cleveland,Boutell,cboutell4@hibu.com,Human Resources,121.174.65.124,cboutell4,6ebZ9J
6,Petronella,Dumbarton,pdumbarton5@hhs.gov,Research and Development,78.40.66.100,pdumbarton5,wKRtpkLnb
7,Katuscha,Pilpovic,kpilpovic6@fastcompany.com,Engineering,169.248.70.125,kpilpovic6,LPJVmy1
8,Jillian,Wiffield,jwiffield7@spotify.com,Support,186.98.209.13,jwiffield7,r4bb8PAX
9,Ermentrude,Lequeux,elequeux8@illinois.edu,Marketing,20.221.162.46,elequeux8,J7wfrg1qNu0
10,Kaine,Hinkens,khinkens9@delicious.com,Legal,211.55.155.211,khinkens9,zBgG5CuOy8s
11,Wade,Johnsey,wjohnseya@gizmodo.com,Accounting,184.85.39.15,wjohnseya,NYh3Kg
12,Reynard,Jacquemy,rjacquemyb@ycombinator.com,Research and Development,132.65.193.167,rjacquemyb,rHiJ1oKf8MJX
13,Karoline,Freeman,kfreemanc@meetup.com,Human Resources,77.34.133.157,kfreemanc,vKLWiWTPa
14,Tracee,Haxby,thaxbyd@auda.org.au,Sales,47.155.61.249,thaxbyd,L5HlAqjsKh89
15,Rochell,Newlove,rnewlovee@sogou.com,Research and Development,242.54.38.46,rnewlovee,Cfia2jDnPOt
16,Eldin,Molyneaux,emolyneauxf@flickr.com,Marketing,143.60.133.71,emolyneauxf,AkMqKLE
17,Annissa,Hallen,ahalleng@npr.org,Services,129.197.253.232,ahalleng,0eYx7o2y1
18,Lowell,Levecque,llevecqueh@chron.com,Marketing,147.84.48.186,llevecqueh,xl59Ksp
19,Ree,Chadwen,rchadweni@wsi.com,Sales,97.119.1.238,rchadweni,PJErRu
```



```
292,Borden,Danilevich,bdanilevich83@oaic.gov.au,Sales,31.164.36.60,bdanilevich83,YKNBcV
```

5.What is the SSH password of the Domain Administrator?

Using the same Alevis_Employee_Information_Chart.csv file, the password of the Domain Admin that is gMR<4eXf]e6W.



```
478,Domain,Admin,DomAdmin@alevis.com,Domain Admin,192.168.56.1,DomAdmin,gMR<4eXf]e6W
```