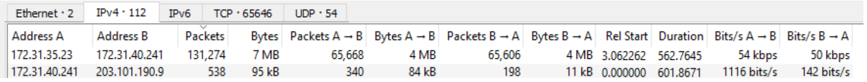
Compromised Network Printer Challenge

You are a DFIR Analyst for a corporation. A network printer running in the internal network has been compromised as it was alerted by our IDS. You have been provided a packet capture to trace the attacker's action and what data was stolen from the printer server.

Task 1:
Identify the port scan activity performed by the attacker on the network. What was the NAT IP Address(Internal IP Address) assigned to the machine being used by the attacker on the internal network?

I checked the Conversation and filtered by packets

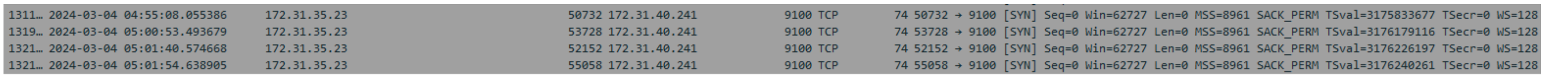


Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
172.31.35.23	172.31.40.241	131,274	7 MB	65,668	4 MB	65,606	4 MB	3.062262	562.7645	54 kbps	50 kbps
172.31.40.241	203.101.190.9	538	95 kB	340	84 kB	198	11 kB	0.000000	601.8671	1116 bits/s	142 bits/s

Answer: 172.31.35.23

Task 2:
Which ports were open on the network printer? Identify the port used for printer exploitation.

I filtered for the attacker IP and SYN packets "ip.src == 172.31.35.23 && tcp.flags.syn == 1 && tcp.flags.ack == 0"
Then I saw port 9100 which is used for printing

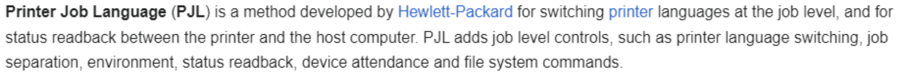


```
1311… 2024-03-04 04:55:08.055386      172.31.35.23                                 50732 172.31.40.241             9100 TCP        74 50732 → 9100 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM TSval=3175833677 TSecr=0 WS=128
1319… 2024-03-04 05:00:53.493679      172.31.35.23                                 53728 172.31.40.241             9100 TCP        74 53728 → 9100 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM TSval=3176179116 TSecr=0 WS=128
1321… 2024-03-04 05:01:40.574668      172.31.35.23                                 52152 172.31.40.241             9100 TCP        74 52152 → 9100 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM TSval=3176226197 TSecr=0 WS=128
1321… 2024-03-04 05:01:54.638905      172.31.35.23                                 55058 172.31.40.241             9100 TCP        74 55058 → 9100 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM TSval=3176240261 TSecr=0 WS=128
```

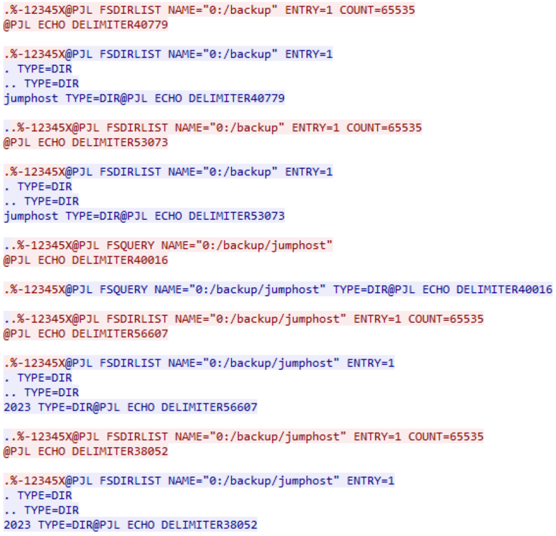
Answer: 9100

Task 3:
Based on the abused port number, which printer language/method was being abused by the attacker for unattended malicious activity on the network printer?

I followed the TCP Stream and noticed that all the commands start with "PJL" (Printer Job Language)



Printer Job Language (**PJL**) is a method developed by Hewlett-Packard for switching printer languages at the job level, and for status readback between the printer and the host computer. PJL adds job level controls, such as printer language switching, job separation, environment, status readback, device attendance and file system commands.

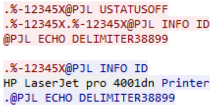


```
.%-12345X@PJL FSDIRLIST NAME="0:/backup" ENTRY=1 COUNT=65535
@PJL ECHO DELIMITER40779

.%-12345X@PJL FSDIRLIST NAME="0:/backup" ENTRY=1
. TYPE=DIR
.. TYPE=DIR
jumphost TYPE=DIR@PJL ECHO DELIMITER40779

..%-12345X@PJL FSDIRLIST NAME="0:/backup" ENTRY=1 COUNT=65535
@PJL ECHO DELIMITER53073

.%-12345X@PJL FSDIRLIST NAME="0:/backup" ENTRY=1
. TYPE=DIR
.. TYPE=DIR
jumphost TYPE=DIR@PJL ECHO DELIMITER53073

..%-12345X@PJL FSQUERY NAME="0:/backup/jumphost"
@PJL ECHO DELIMITER40016

.%-12345X@PJL FSQUERY NAME="0:/backup/jumphost" TYPE=DIR@PJL ECHO DELIMITER40016

..%-12345X@PJL FSDIRLIST NAME="0:/backup/jumphost" ENTRY=1 COUNT=65535
@PJL ECHO DELIMITER56607

.%-12345X@PJL FSDIRLIST NAME="0:/backup/jumphost" ENTRY=1
. TYPE=DIR
.. TYPE=DIR
2023 TYPE=DIR@PJL ECHO DELIMITER56607

..%-12345X@PJL FSDIRLIST NAME="0:/backup/jumphost" ENTRY=1 COUNT=65535
@PJL ECHO DELIMITER38052

.%-12345X@PJL FSDIRLIST NAME="0:/backup/jumphost" ENTRY=1
. TYPE=DIR
.. TYPE=DIR
2023 TYPE=DIR@PJL ECHO DELIMITER38052
```

Answer: PJL

Task 4:
Which Printer Name/Model was attacked?

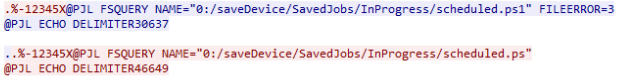
I followed another TCP Stream with the port 9100 and found the model



```
.%-12345X@PJL USTATUSOFF
.%-12345X.%-12345X@PJL INFO ID
@PJL ECHO DELIMITER38899

.%-12345X@PJL INFO ID
HP LaserJet pro 4001dn Printer
.@PJL ECHO DELIMITER38899
```

Task 5:
The attacker has discovered a scheduled print job that is associated with an employee who is suspected
of being an insider threat. What is the full path of the print job file?

From same TCP Stream like task 4, I saw the something with scheduled

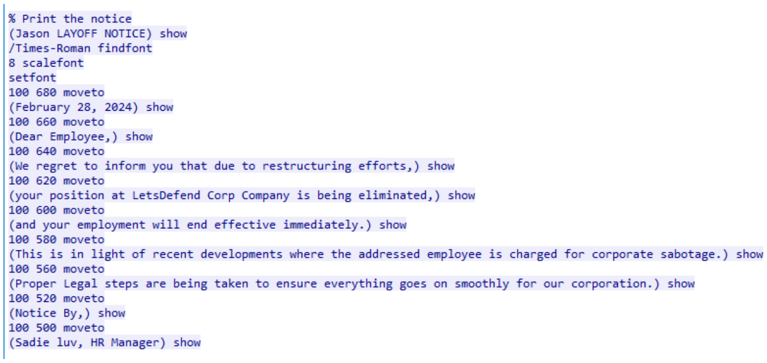


```
.%-12345X@PJL FSQUERY NAME="0:/saveDevice/SavedJobs/InProgress/scheduled.ps1" FILEERROR=3
@PJL ECHO DELIMITER30637

..%-12345X@PJL FSQUERY NAME="0:/saveDevice/SavedJobs/InProgress/scheduled.ps"
@PJL ECHO DELIMITER46649
```

Answer: 0:/saveDevice/SavedJobs/InProgress/scheduled.ps

Task 6:
What is the name of the targeted organization?

I found the name inside the TCP stream while I found the schedules.ps in task 5

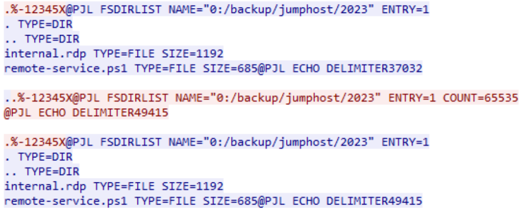


```
% Print the notice
(Jason LAYOFF NOTICE) show
/Times-Roman findfont
8 scalefont
setfont
100 680 moveto
(February 28, 2024) show
100 660 moveto
(Dear Employee,) show
100 640 moveto
(We regret to inform you that due to restructuring efforts,) show
100 620 moveto
(your position at LetsDefend Corp Company is being eliminated,) show
100 600 moveto
(and your employment will end effective immediately.) show
100 580 moveto
(This is in light of recent developments where the addressed employee is charged for corporate sabotage.) show
100 560 moveto
(Proper Legal steps are being taken to ensure everything goes on smoothly for our corporation.) show
100 520 moveto
(Notice By,) show
100 500 moveto
(Sadie luv, HR Manager) show
```

Answer: LetsDefend Corp Company

Task 7:
The attacker found information about RDP within the internal network. What is the directory path
where this sensitive information was located?

I found this from the same TCP Stream in task 3

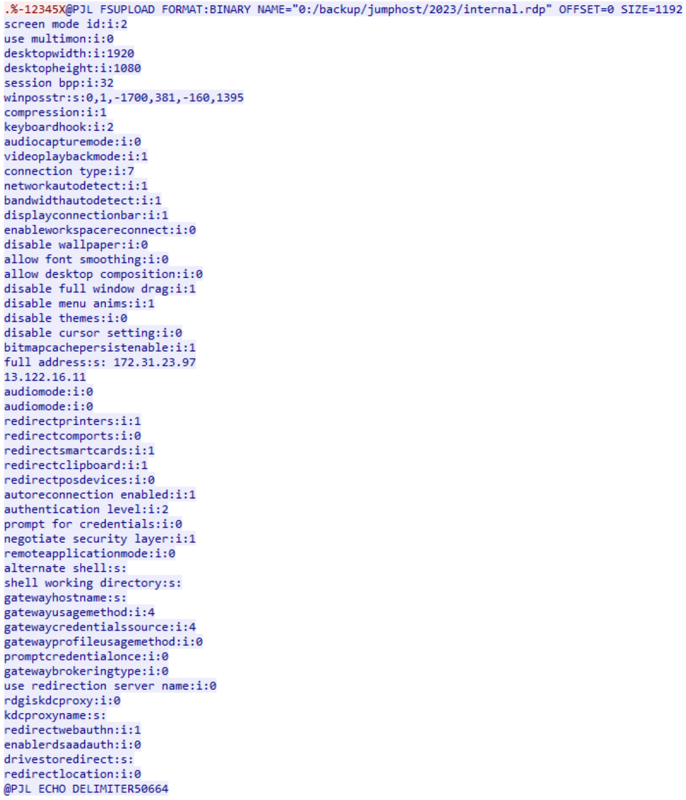


```
.%-12345X@PJL FSDIRLIST NAME="0:/backup/jumphost/2023" ENTRY=1
. TYPE=DIR
.. TYPE=DIR
internal.rdp TYPE=FILE SIZE=1192
remote-service.ps1 TYPE=FILE SIZE=685@PJL ECHO DELIMITER37032

..%-12345X@PJL FSDIRLIST NAME="0:/backup/jumphost/2023" ENTRY=1 COUNT=65535
@PJL ECHO DELIMITER49415

.%-12345X@PJL FSDIRLIST NAME="0:/backup/jumphost/2023" ENTRY=1
. TYPE=DIR
.. TYPE=DIR
internal.rdp TYPE=FILE SIZE=1192
remote-service.ps1 TYPE=FILE SIZE=685@PJL ECHO DELIMITER49415
```

Answer: /backup/jumphost/2023

Task 8:
What is the IP address of the Jumphost?

Same as the previous tasks, found this from the TCP Stream

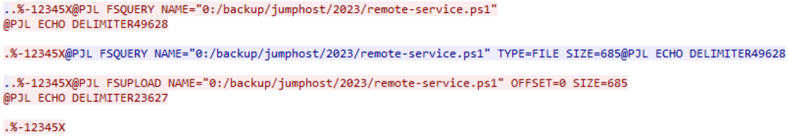


```
.%-12345X@PJL FSUPLOAD FORMAT:BINARY NAME="0:/backup/jumphost/2023/internal.rdp" OFFSET=0 SIZE=1192
screen mode id:i:2
use multimon:i:0
desktopwidth:i:1920
desktopheight:i:1080
session bpp:i:32
winposstr:s:0,1,-1700,381,-160,1395
compression:i:1
keyboardhook:i:2
audiocapturemode:i:0
videoplaybackmode:i:1
connection type:i:7
networkautodetect:i:1
bandwidthautodetect:i:1
displayconnectionbar:i:1
enableworkspacereconnect:i:0
disable wallpaper:i:0
allow font smoothing:i:0
allow desktop composition:i:0
disable full window drag:i:1
disable menu anims:i:1
disable themes:i:0
disable cursor setting:i:0
bitmapcachepersistenable:i:1
full address:s: 172.31.23.97
13.122.16.11
audiomode:i:0
audiomode:i:0
redirectprinters:i:1
redirectcomports:i:0
redirectsmartcards:i:1
redirectclipboard:i:1
redirectposdevices:i:0
autoreconnection enabled:i:1
authentication level:i:2
prompt for credentials:i:0
negotiate security layer:i:1
remoteapplicationmode:i:0
alternate shell:s:
shell working directory:s:
gatewayhostname:s:
gatewayusagemethod:i:4
gatewaycredentialssource:i:4
gatewayprofileusagemethod:i:0
promptcredentialonce:i:0
gatewaybrokeringtype:i:0
use redirection server name:i:0
rdgiskdcproxy:i:0
kdcproxyname:s:
redirectwebauthn:i:1
enablerdsaadauth:i:0
drivestoredirect:s:
redirectlocation:i:0
@PJL ECHO DELIMITER50664
```

Answer: 172.31.23.97

Task 9:
What is the filename of the PowerShell script used by admins which was also found by the attacker?

From same TCP Stream in task 9 I saw the script



```
..%-12345X@PJL FSQUERY NAME="0:/backup/jumphost/2023/remote-service.ps1"
@PJL ECHO DELIMITER49628

.%-12345X@PJL FSQUERY NAME="0:/backup/jumphost/2023/remote-service.ps1" TYPE=FILE SIZE=685@PJL ECHO DELIMITER49628

..%-12345X@PJL FSUPLOAD NAME="0:/backup/jumphost/2023/remote-service.ps1" OFFSET=0 SIZE=685
@PJL ECHO DELIMITER23627

.%-12345X
```

Answer: remote-service.ps1