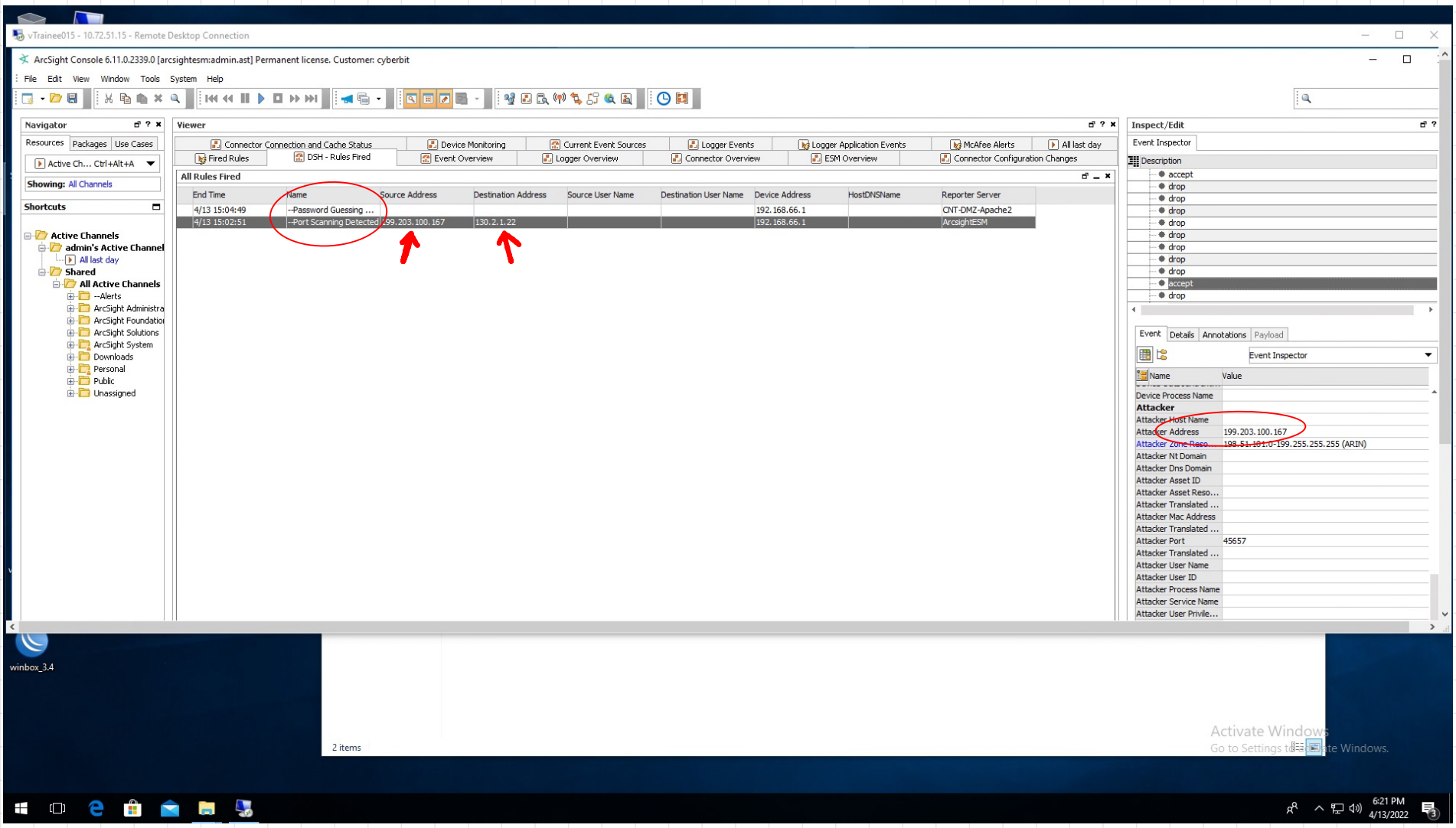
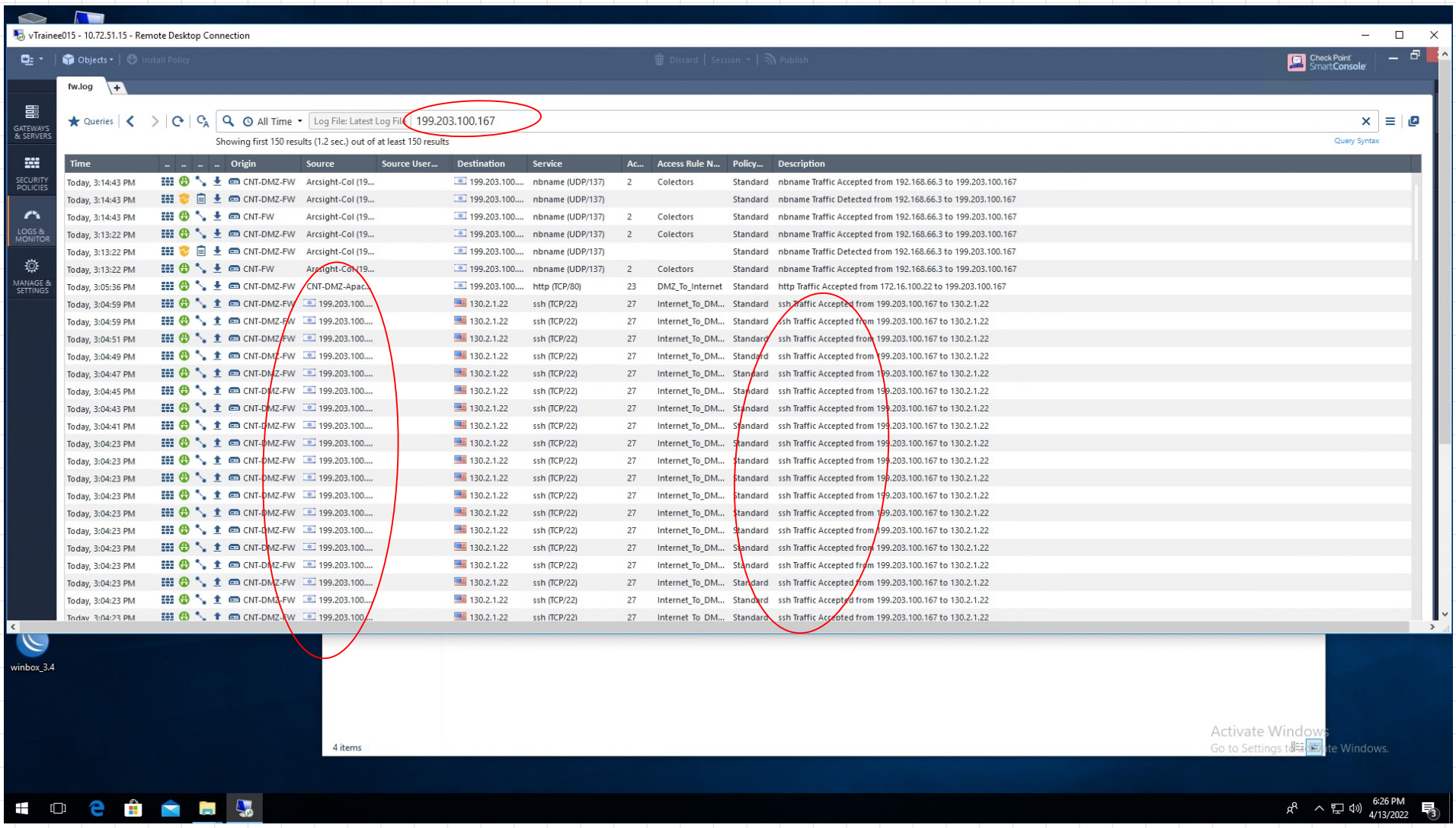


4.13 בשעה 15:04 קיבלנו התרעה ב-ArcSight שמכתובת ה-IP 199.203.100.167 מישהו ניסה לנחש את הסיסמה(Password Guessing) ואז התחיל לסרוק פורטים(Port Scanning Detected) ב130.2.1.22 ip ש זה NAT 172.16.100.22

סרקת פורטים-דרך לזהות צמתים פגיעים ברשת על ידי גישה ליציאות שונות במארח (התקן המחובר לרשת) או לאותה יציאה במארחים שונים. זה יכול לשמש תוקפים בשלב ההכנה של המתקפה כדי לאסוף מידע על מארח היעד, כמו גם על ידי מומחי אבטחה ככלי לאיתור נקודות תורפה בתשתית ה-IT.



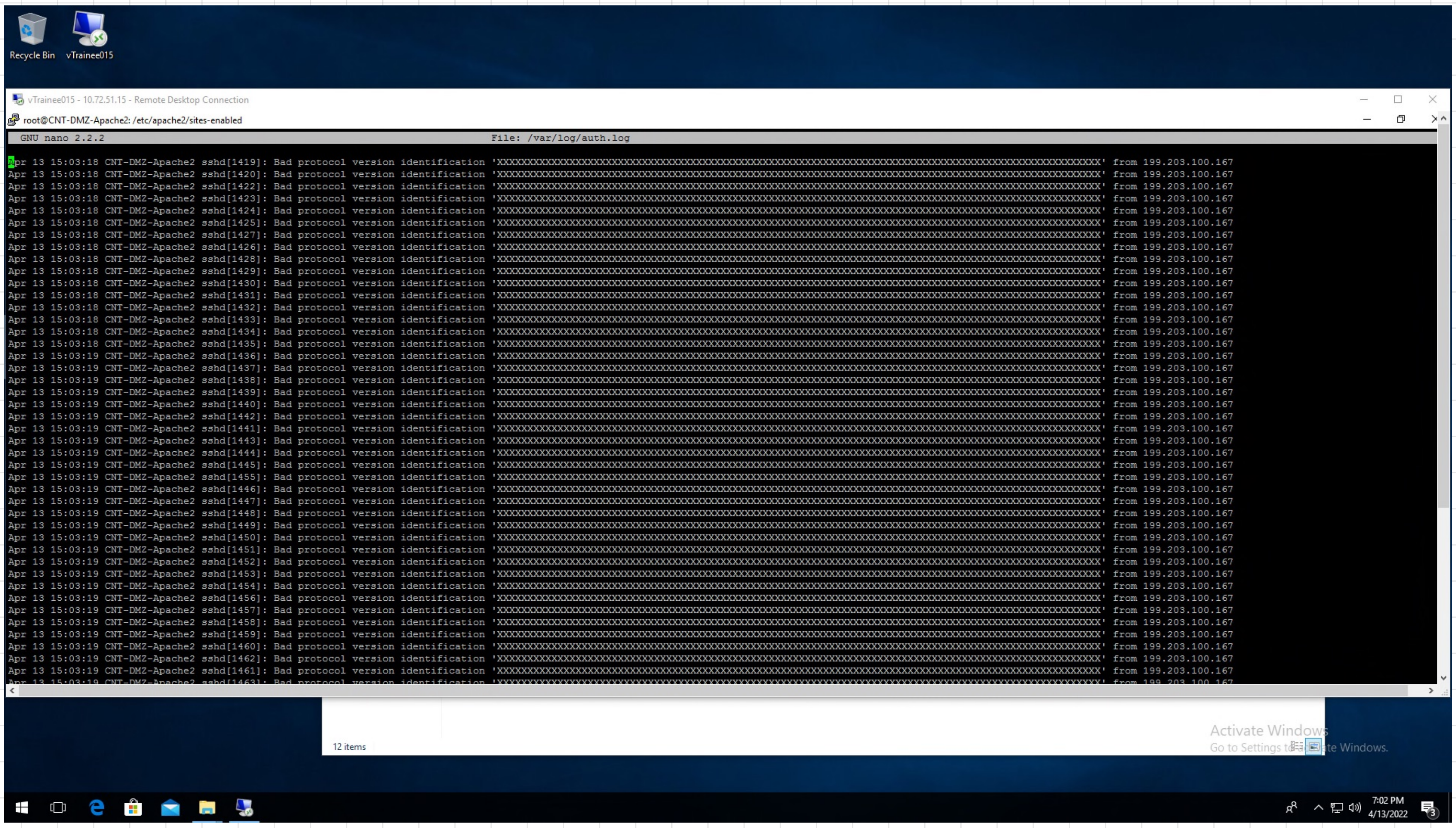
אנחנו לא יודעים אם הוא הצליח להתחבר על ידי ניחוש הסיסמה, ואנחנו הולכים ל-SmartConsole וכתוב ip של התוקף . ואנו רואים מספר רב של בקשות להתחבר מרחוק באמצעות ssh.

ואז הלכנו ל-ip של השרת וראינו שהוא נפרץ והנתונים הוחלפו באחרים

```
root@CNT-DMZ-Apache2:~# netstat -tuna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN
tcp        0      0 172.16.100.22:22        199.203.100.66:37867    ESTABLISHED
tcp        0      0 172.16.100.22:22        192.168.110.110:55472   ESTABLISHED
tcp6       0      0 :::22                   :::*                    LISTEN
udp        0      0 0.0.0.0:55375           0.0.0.0:*
udp        0      0 0.0.0.0:514             0.0.0.0:*
udp        0      0 0.0.0.0:41093           0.0.0.0:*
udp        0      0 0.0.0.0:161             0.0.0.0:*
udp6       0      0 :::514                  :::*
```

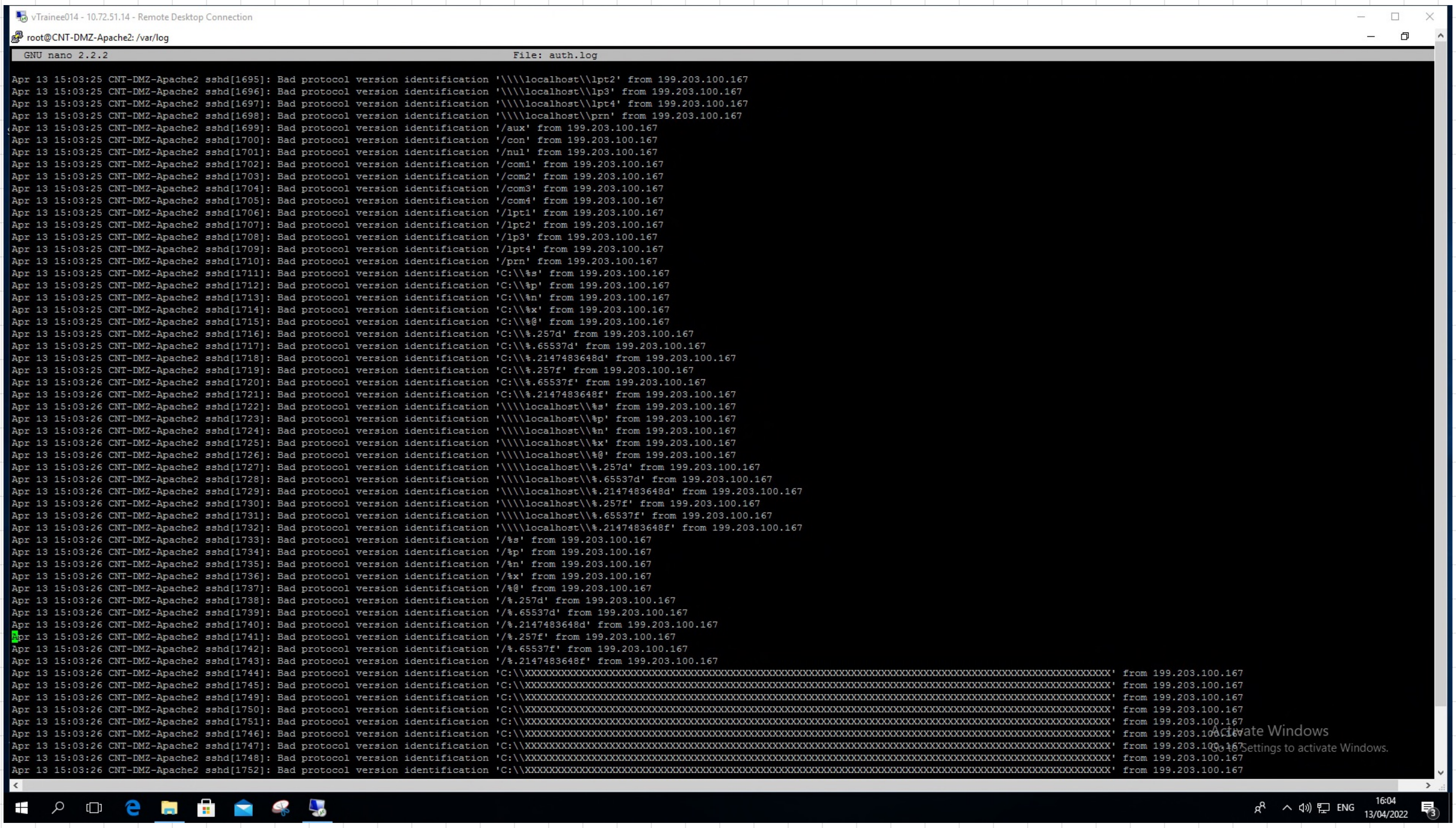
התחברנו לשרת באמצעות מרק כדי לברר אם הוא מחובר כעת. אנו רואים שמישהו התחבר אלינו דרך פורט 22

עכשיו אנחנו עוברים ללוג (var/log/auth.log)



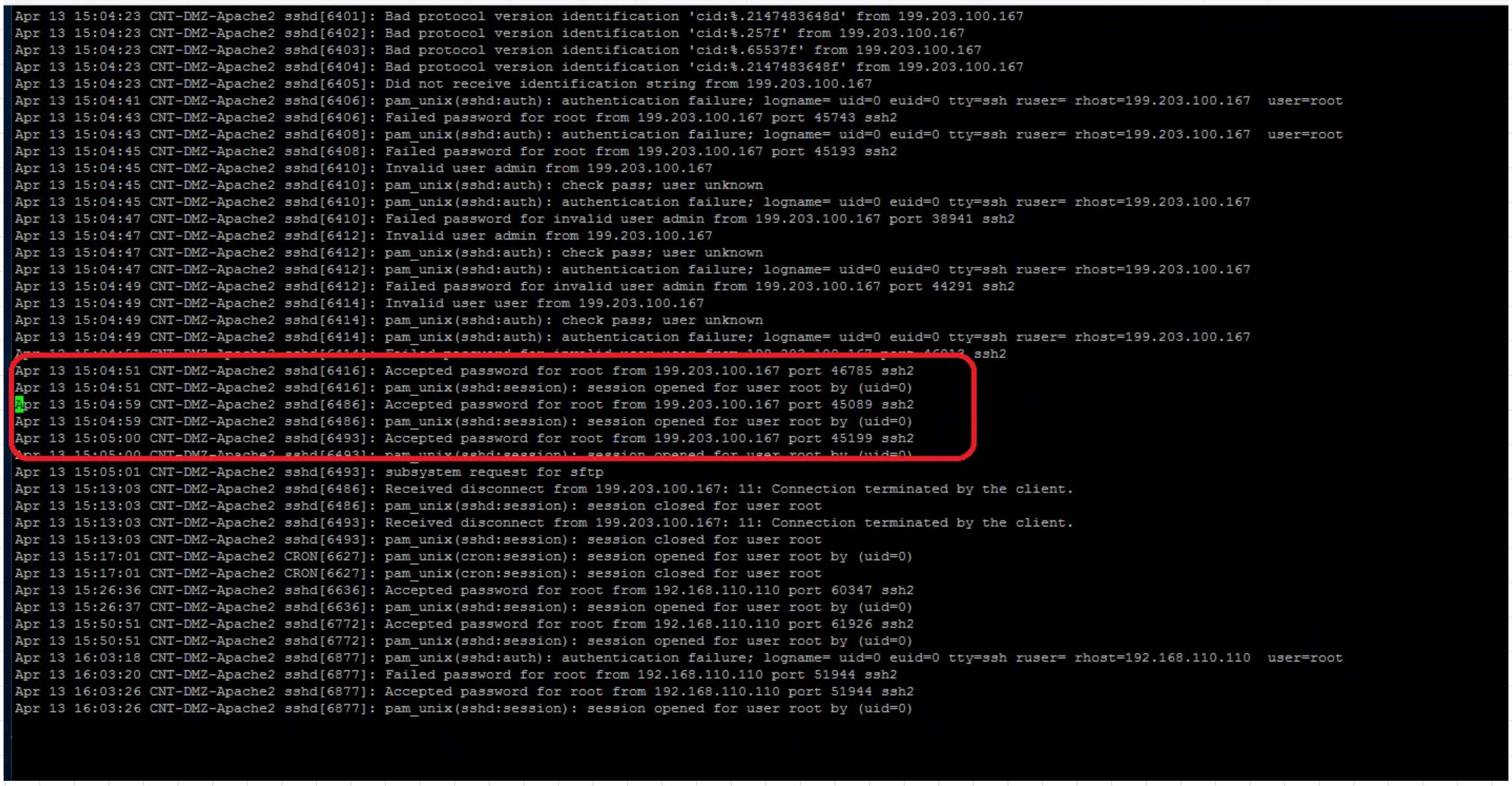
```
  GNU nano 2.2.2                                       File: /var/log/auth.log

Apr 13 15:03:18 CNT-DMZ-Apache2 sshd[1419]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:18 CNT-DMZ-Apache2 sshd[1420]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:18 CNT-DMZ-Apache2 sshd[1422]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:18 CNT-DMZ-Apache2 sshd[1423]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:18 CNT-DMZ-Apache2 sshd[1424]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:18 CNT-DMZ-Apache2 sshd[1425]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:18 CNT-DMZ-Apache2 sshd[1427]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:18 CNT-DMZ-Apache2 sshd[1426]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:18 CNT-DMZ-Apache2 sshd[1428]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:18 CNT-DMZ-Apache2 sshd[1429]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:18 CNT-DMZ-Apache2 sshd[1430]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:18 CNT-DMZ-Apache2 sshd[1431]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:18 CNT-DMZ-Apache2 sshd[1432]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:18 CNT-DMZ-Apache2 sshd[1433]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:18 CNT-DMZ-Apache2 sshd[1434]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:18 CNT-DMZ-Apache2 sshd[1435]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:19 CNT-DMZ-Apache2 sshd[1436]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:19 CNT-DMZ-Apache2 sshd[1437]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:19 CNT-DMZ-Apache2 sshd[1438]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:19 CNT-DMZ-Apache2 sshd[1439]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:19 CNT-DMZ-Apache2 sshd[1440]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:19 CNT-DMZ-Apache2 sshd[1442]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:19 CNT-DMZ-Apache2 sshd[1441]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:19 CNT-DMZ-Apache2 sshd[1443]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:19 CNT-DMZ-Apache2 sshd[1444]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:19 CNT-DMZ-Apache2 sshd[1445]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:19 CNT-DMZ-Apache2 sshd[1455]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:19 CNT-DMZ-Apache2 sshd[1446]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:19 CNT-DMZ-Apache2 sshd[1447]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:19 CNT-DMZ-Apache2 sshd[1448]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:19 CNT-DMZ-Apache2 sshd[1449]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:19 CNT-DMZ-Apache2 sshd[1450]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:19 CNT-DMZ-Apache2 sshd[1451]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:19 CNT-DMZ-Apache2 sshd[1452]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:19 CNT-DMZ-Apache2 sshd[1453]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:19 CNT-DMZ-Apache2 sshd[1454]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:19 CNT-DMZ-Apache2 sshd[1456]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:19 CNT-DMZ-Apache2 sshd[1457]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:19 CNT-DMZ-Apache2 sshd[1458]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:19 CNT-DMZ-Apache2 sshd[1459]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:19 CNT-DMZ-Apache2 sshd[1460]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:19 CNT-DMZ-Apache2 sshd[1462]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:19 CNT-DMZ-Apache2 sshd[1461]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:19 CNT-DMZ-Apache2 sshd[1463]: Bad protocol version identification 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
```



```
  GNU nano 2.2.2                                       File: auth.log

Apr 13 15:03:25 CNT-DMZ-Apache2 sshd[1695]: Bad protocol version identification '\\\\localhost\\lpt2' from 199.203.100.167
Apr 13 15:03:25 CNT-DMZ-Apache2 sshd[1696]: Bad protocol version identification '\\\\localhost\\lp3' from 199.203.100.167
Apr 13 15:03:25 CNT-DMZ-Apache2 sshd[1697]: Bad protocol version identification '\\\\localhost\\lpt4' from 199.203.100.167
Apr 13 15:03:25 CNT-DMZ-Apache2 sshd[1698]: Bad protocol version identification '\\\\localhost\\prn' from 199.203.100.167
Apr 13 15:03:25 CNT-DMZ-Apache2 sshd[1699]: Bad protocol version identification '/aux' from 199.203.100.167
Apr 13 15:03:25 CNT-DMZ-Apache2 sshd[1700]: Bad protocol version identification '/con' from 199.203.100.167
Apr 13 15:03:25 CNT-DMZ-Apache2 sshd[1701]: Bad protocol version identification '/nul' from 199.203.100.167
Apr 13 15:03:25 CNT-DMZ-Apache2 sshd[1702]: Bad protocol version identification '/com1' from 199.203.100.167
Apr 13 15:03:25 CNT-DMZ-Apache2 sshd[1703]: Bad protocol version identification '/com2' from 199.203.100.167
Apr 13 15:03:25 CNT-DMZ-Apache2 sshd[1704]: Bad protocol version identification '/com3' from 199.203.100.167
Apr 13 15:03:25 CNT-DMZ-Apache2 sshd[1705]: Bad protocol version identification '/com4' from 199.203.100.167
Apr 13 15:03:25 CNT-DMZ-Apache2 sshd[1706]: Bad protocol version identification '/lpt1' from 199.203.100.167
Apr 13 15:03:25 CNT-DMZ-Apache2 sshd[1707]: Bad protocol version identification '/lpt2' from 199.203.100.167
Apr 13 15:03:25 CNT-DMZ-Apache2 sshd[1708]: Bad protocol version identification '/lp3' from 199.203.100.167
Apr 13 15:03:25 CNT-DMZ-Apache2 sshd[1709]: Bad protocol version identification '/lpt4' from 199.203.100.167
Apr 13 15:03:25 CNT-DMZ-Apache2 sshd[1710]: Bad protocol version identification '/prn' from 199.203.100.167
Apr 13 15:03:25 CNT-DMZ-Apache2 sshd[1711]: Bad protocol version identification 'C:\\%s' from 199.203.100.167
Apr 13 15:03:25 CNT-DMZ-Apache2 sshd[1712]: Bad protocol version identification 'C:\\%p' from 199.203.100.167
Apr 13 15:03:25 CNT-DMZ-Apache2 sshd[1713]: Bad protocol version identification 'C:\\%n' from 199.203.100.167
Apr 13 15:03:25 CNT-DMZ-Apache2 sshd[1714]: Bad protocol version identification 'C:\\%x' from 199.203.100.167
Apr 13 15:03:25 CNT-DMZ-Apache2 sshd[1715]: Bad protocol version identification 'C:\\%@' from 199.203.100.167
Apr 13 15:03:25 CNT-DMZ-Apache2 sshd[1716]: Bad protocol version identification 'C:\\%.257d' from 199.203.100.167
Apr 13 15:03:25 CNT-DMZ-Apache2 sshd[1717]: Bad protocol version identification 'C:\\%.65537d' from 199.203.100.167
Apr 13 15:03:25 CNT-DMZ-Apache2 sshd[1718]: Bad protocol version identification 'C:\\%.2147483648d' from 199.203.100.167
Apr 13 15:03:25 CNT-DMZ-Apache2 sshd[1719]: Bad protocol version identification 'C:\\%.257f' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1720]: Bad protocol version identification 'C:\\%.65537f' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1721]: Bad protocol version identification 'C:\\%.2147483648f' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1722]: Bad protocol version identification '\\\\localhost\\%s' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1723]: Bad protocol version identification '\\\\localhost\\%p' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1724]: Bad protocol version identification '\\\\localhost\\%n' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1725]: Bad protocol version identification '\\\\localhost\\%x' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1726]: Bad protocol version identification '\\\\localhost\\%@' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1727]: Bad protocol version identification '\\\\localhost\\%.257d' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1728]: Bad protocol version identification '\\\\localhost\\%.65537d' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1729]: Bad protocol version identification '\\\\localhost\\%.2147483648d' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1730]: Bad protocol version identification '\\\\localhost\\%.257f' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1731]: Bad protocol version identification '\\\\localhost\\%.65537f' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1732]: Bad protocol version identification '\\\\localhost\\%.2147483648f' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1733]: Bad protocol version identification '/%s' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1734]: Bad protocol version identification '/%p' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1735]: Bad protocol version identification '/%n' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1736]: Bad protocol version identification '/%x' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1737]: Bad protocol version identification '/%@' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1738]: Bad protocol version identification '/%.257d' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1739]: Bad protocol version identification '/%.65537d' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1740]: Bad protocol version identification '/%.2147483648d' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1741]: Bad protocol version identification '/%.257f' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1742]: Bad protocol version identification '/%.65537f' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1743]: Bad protocol version identification '/%.2147483648f' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1744]: Bad protocol version identification 'C:\\XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1745]: Bad protocol version identification 'C:\\XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1749]: Bad protocol version identification 'C:\\XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1750]: Bad protocol version identification 'C:\\XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1751]: Bad protocol version identification 'C:\\XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1746]: Bad protocol version identification 'C:\\XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1747]: Bad protocol version identification 'C:\\XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1748]: Bad protocol version identification 'C:\\XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
Apr 13 15:03:26 CNT-DMZ-Apache2 sshd[1752]: Bad protocol version identification 'C:\\XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' from 199.203.100.167
```



```
Apr 13 15:04:23 CNT-DMZ-Apache2 sshd[6401]: Bad protocol version identification 'cid:%.2147483648d' from 199.203.100.167
Apr 13 15:04:23 CNT-DMZ-Apache2 sshd[6402]: Bad protocol version identification 'cid:%.257f' from 199.203.100.167
Apr 13 15:04:23 CNT-DMZ-Apache2 sshd[6403]: Bad protocol version identification 'cid:%.65537f' from 199.203.100.167
Apr 13 15:04:23 CNT-DMZ-Apache2 sshd[6404]: Bad protocol version identification 'cid:%.2147483648f' from 199.203.100.167
Apr 13 15:04:23 CNT-DMZ-Apache2 sshd[6405]: Did not receive identification string from 199.203.100.167
Apr 13 15:04:41 CNT-DMZ-Apache2 sshd[6406]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=199.203.100.167  user=root
Apr 13 15:04:43 CNT-DMZ-Apache2 sshd[6406]: Failed password for root from 199.203.100.167 port 45743 ssh2
Apr 13 15:04:43 CNT-DMZ-Apache2 sshd[6408]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=199.203.100.167  user=root
Apr 13 15:04:45 CNT-DMZ-Apache2 sshd[6408]: Failed password for root from 199.203.100.167 port 45193 ssh2
Apr 13 15:04:45 CNT-DMZ-Apache2 sshd[6410]: Invalid user admin from 199.203.100.167
Apr 13 15:04:45 CNT-DMZ-Apache2 sshd[6410]: pam_unix(sshd:auth): check pass; user unknown
Apr 13 15:04:45 CNT-DMZ-Apache2 sshd[6410]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=199.203.100.167
Apr 13 15:04:47 CNT-DMZ-Apache2 sshd[6410]: Failed password for invalid user admin from 199.203.100.167 port 38941 ssh2
Apr 13 15:04:47 CNT-DMZ-Apache2 sshd[6412]: Invalid user admin from 199.203.100.167
Apr 13 15:04:47 CNT-DMZ-Apache2 sshd[6412]: pam_unix(sshd:auth): check pass; user unknown
Apr 13 15:04:47 CNT-DMZ-Apache2 sshd[6412]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=199.203.100.167
Apr 13 15:04:49 CNT-DMZ-Apache2 sshd[6412]: Failed password for invalid user admin from 199.203.100.167 port 44291 ssh2
Apr 13 15:04:49 CNT-DMZ-Apache2 sshd[6414]: Invalid user user from 199.203.100.167
Apr 13 15:04:49 CNT-DMZ-Apache2 sshd[6414]: pam_unix(sshd:auth): check pass; user unknown
Apr 13 15:04:49 CNT-DMZ-Apache2 sshd[6414]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=199.203.100.167
Apr 13 15:04:51 CNT-DMZ-Apache2 sshd[6414]: Failed password for invalid user user from 199.203.100.167 port 46013 ssh2
Apr 13 15:04:51 CNT-DMZ-Apache2 sshd[6416]: Accepted password for root from 199.203.100.167 port 46785 ssh2
Apr 13 15:04:51 CNT-DMZ-Apache2 sshd[6416]: pam_unix(sshd:session): session opened for user root by (uid=0)
Apr 13 15:04:59 CNT-DMZ-Apache2 sshd[6486]: Accepted password for root from 199.203.100.167 port 45089 ssh2
Apr 13 15:04:59 CNT-DMZ-Apache2 sshd[6486]: pam_unix(sshd:session): session opened for user root by (uid=0)
Apr 13 15:05:00 CNT-DMZ-Apache2 sshd[6493]: Accepted password for root from 199.203.100.167 port 45199 ssh2
Apr 13 15:05:00 CNT-DMZ-Apache2 sshd[6493]: pam_unix(sshd:session): session opened for user root by (uid=0)
Apr 13 15:05:01 CNT-DMZ-Apache2 sshd[6493]: subsystem request for sftp
Apr 13 15:13:03 CNT-DMZ-Apache2 sshd[6486]: Received disconnect from 199.203.100.167: 11: Connection terminated by the client.
Apr 13 15:13:03 CNT-DMZ-Apache2 sshd[6486]: pam_unix(sshd:session): session closed for user root
Apr 13 15:13:03 CNT-DMZ-Apache2 sshd[6493]: Received disconnect from 199.203.100.167: 11: Connection terminated by the client.
Apr 13 15:13:03 CNT-DMZ-Apache2 sshd[6493]: pam_unix(sshd:session): session closed for user root
Apr 13 15:17:01 CNT-DMZ-Apache2 CRON[6627]: pam_unix(cron:session): session opened for user root by (uid=0)
Apr 13 15:17:01 CNT-DMZ-Apache2 CRON[6627]: pam_unix(cron:session): session closed for user root
Apr 13 15:26:36 CNT-DMZ-Apache2 sshd[6636]: Accepted password for root from 192.168.110.110 port 60347 ssh2
Apr 13 15:26:37 CNT-DMZ-Apache2 sshd[6636]: pam_unix(sshd:session): session opened for user root by (uid=0)
Apr 13 15:50:51 CNT-DMZ-Apache2 sshd[6772]: Accepted password for root from 192.168.110.110 port 61926 ssh2
Apr 13 15:50:51 CNT-DMZ-Apache2 sshd[6772]: pam_unix(sshd:session): session opened for user root by (uid=0)
Apr 13 16:03:18 CNT-DMZ-Apache2 sshd[6877]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.110.110  user=root
Apr 13 16:03:20 CNT-DMZ-Apache2 sshd[6877]: Failed password for root from 192.168.110.110 port 51944 ssh2
Apr 13 16:03:26 CNT-DMZ-Apache2 sshd[6877]: Accepted password for root from 192.168.110.110 port 51944 ssh2
Apr 13 16:03:26 CNT-DMZ-Apache2 sshd[6877]: pam_unix(sshd:session): session opened for user root by (uid=0)
```

ראינו הרבה ניסיונות
bad protocol version indetification עם
fuzzing והבנו שזה

טכניקת בדיקת תוכנה, לרוב אוטומטית או חצי אוטומטית, שבה נתונים שגויים, בלתי צפויים או אקראיים מועברים לאפליקציה כקלט. נושא העניין הוא קריסות והקפאות, הפרות של לוגיקה פנימית ובדיקות בקוד האפליקציה, דליפות זיכרון הנגרמות על ידי נתוני קלט כאלה. Fuzzing הוא סוג של בדיקות אקראיות המשמשות לעתים קרובות כדי לבדוק בעיות אבטחה בתוכנה ובמערכות מחשב.

והתחלנו לחפש בשרת את שם הקובץ הזה.
מצאנו את זה

```
root@CNT-DMZ-Apache2:/var/log# find / -name "hacked2z.png"
/var/www/BBC/hacked2z.png
```

נכנסנו לתיקיית var/www וראינו שיש שם 2 תיקיות:
bbc ו- bbc ישן

```
root@CNT-DMZ-Apache2:/var/www/BBC# cd ..
root@CNT-DMZ-Apache2:/var/www# ls
BBC  BBC_old
```

ותמונתו של התוקף נמצאת בתיקיית ה-BBC

```
root@CNT-DMZ-Apache2:/var# cd www/BBC
root@CNT-DMZ-Apache2:/var/www/BBC# ls
6live                b                  dc                  hacked2z.png        index-9.html        c021d.g
7110                 b17e3.gif          desktopfavicon.png  health              index.html          c03d5.g
7113                 backblue.gif       em_image.gif        help                iplayer             c05d4.g
7127                 bbc                emp                 history             js                  c0e45.g
7251                 bbc.com            espncricinfo        hts-cache           learning            c0fad.g
7259                 bbcdotcom          f                   hts-log.txt         le-tour             c104f.g
7278                 BBCSport.html      fade.gif            idcta               local               c113c.gi
8022                 bbcsportwebsite    favicon.gif         img                 locator             c1383.gi
8146                 blogs              favicon.ico         index-10.html       media               c15bc.gi
8284                 cbb                favicon.ie9new.ico  index-10.html.readme mobile             c176b.gi
8285                 cbbc               favicon.png         index-2.html        modules             c1954.gi
8432                 cbeebies           favicons            index-3.html        music               c1cfe.gi
a                    cgi-bin            flash               index4ec2.html      nature              c1f32.gi
aboutthebbc          comedy             food                index4ec2.html.readme naturelibrary     c21ce.gif
accessibility        cookies.txt        frameworks          index-4.html        navigation          c2350.gif
andrewbensonf1.html  corporate          future              index-5.html        news                c275b.gif
arabic               css                gateway             index-6.html        nol                 c27d1.gif
assets               dartproxy          glow                index-7.html        N5ff24.html         c2957.gif
a-z                  db                 guidance            index-8.html        N5ff24.html.readme  c2b51.gif
```

מחקנו את התיקיה BBC, ואז שינינו את שם התיקיה BBC_old ל-BBC
ושרת חזר לעבוד