Packet Analysis using Wireshark

I have this packet using the wireshark open source tools and this tools is mostly present in the os such as Parrot os and kali linux

first load the pcap file into the wireshark and filter to only http traffic so that u can only see the http traffic

Sub-task 1:

- *anz-logo.jpg and bank-card.jpg are two images that show up in the users network traffic.*
- *Extract these images from the pcap file and attach them to your report.*

First filter the packet capture for http traffic and looked through the remaining packets for the GET request that downloaded the image. than follow the tcp stream and the jpeg file signatures starts with the “FFD8” at the top and the footer will be “FFD9” copy the hex data save the file as jpg format and render it

Sub-task 2:

- *The network traffic for the images "ANZ1.jpg" and "ANZ2.jpg" is more than it appears.*
- *Extract the images, include them and mention what is different about them in your report.*

Follow the same procedure as above and we will end up with this image below
but while finding this image we will get an hidden message “You've found a hidden message in this file! Include it in your write up.”

PROTECT YOUR VIRTUAL VALUABLES

TAKE SOME SIMPLE STEPS TO PROTECT YOUR INFORMATION

ANZ Cyber Secure

ANZ

MAKE A 'PACT'

TO PROTECT YOUR VIRTUAL VALUABLES

PAUSE
before sharing your personal information

Ask yourself, do I really need to give my information to this website or this person? If it doesn't feel right, don't share it.

CALL OUT
suspicious messages

Be aware of current scams. If an email, call or SMS seems unusual, check it through official contact points or report it.

ACTIVATE
two layers of security with two-factor authentication

Use two-factor authentication for an extra layer of security to keep your personal information safe.

TURN ON
automatic software updates

Set your software, operating system and apps to auto update to make sure you get the latest security features.

Report suspicious messages from ANZ:

Email hoax@cybersecurity.anz.com

Report fraudulent or unusual ANZ account activity:

137 028 / +61 3 8693 7153 (Corporate/Business Clients)

133 350 / +61 3 9683 8833 (Personal Banking Customers)

Australia and New Zealand Banking Group Limited (ANZ) ABN 11 005 357 522. Item No. 961848 09.2018 AU22349

Even after finding this image we will get an hidden image “ You've found the hidden message! Images are sometimes more than they appear.”

Sub-task 3:

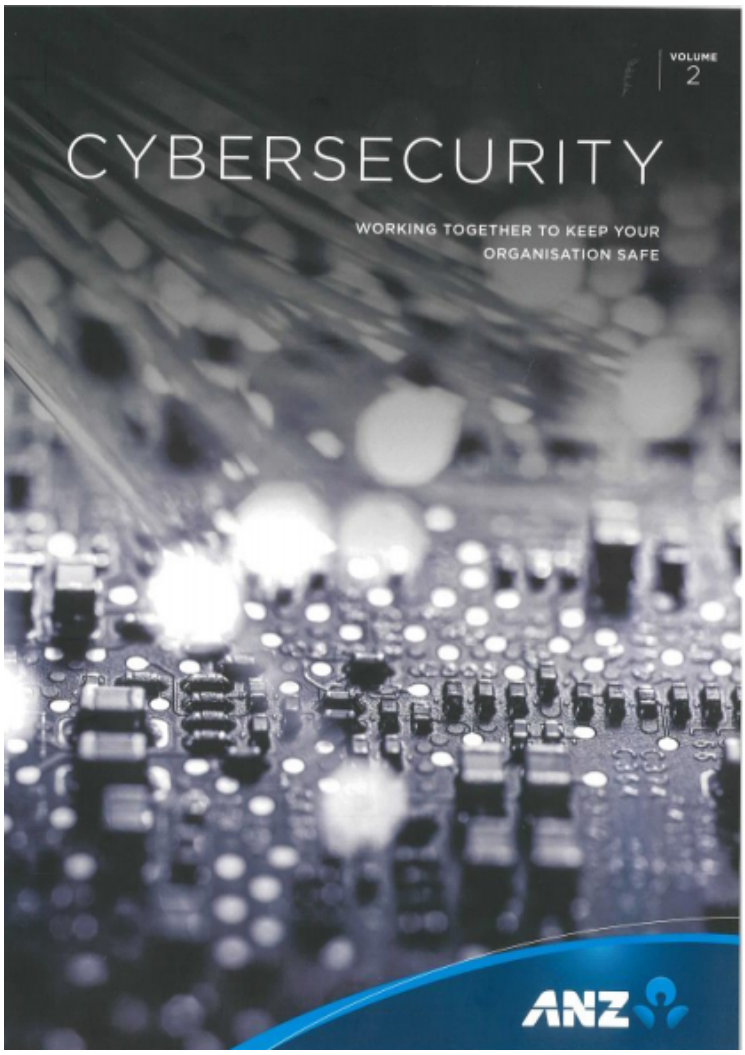
- *The user downloaded a suspicious document called "how-to-commit-crimes.docx"*
- *Find the contents of this file and include it in your report.*
  First follow the TCP stream of the HTTP GET request for the pcap file and view them in the ASCII format
  Step 1: Find target
  Step 2: Hack them
  This is a suspicious document

```
GET /how-to-commit-crimes.docx HTTP/1.1
Host: localhost:8000
Connection: keep-alive
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.100 Safari/
537.36
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
Date: Fri, 16 Aug 2019 00:48:17 GMT
Server: Apache/2.4.6 (CentOS)
Last-Modified: Mon, 05 Aug 2019 02:23:32 GMT
ETag: "46-58f5564f85059"
Accept-Ranges: bytes
Content-Length: 70
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/vnd.openxmlformats-officedocument.wordprocessingml.document

Step 1: Find target
Step 2: Hack them

This is a suspicious document.
```

Sub-task 4:

- *The user accessed 3 pdf documents: ANZ_Document.pdf, ANZ_Document2.pdf, evil.pdf*
- *Extract and view these documents. Include images of them in your report.*

In order to view these PDF's I viewed the TCP stream as usual, and found the file signature for a PDF, which was the hex data "25 50 44 46". I noticed in the ASCII view that the PDF data went until the very end of the TCP stream, so I copied all the hex data from the file signature onwards into HxD and saved it as a pdf file. The same process worked for all three files



THE CHANGING CYBER THREAT LANDSCAPE

COMMON ATTACK VECTORS

AT A GLANCE

- Cybercriminals exploit any weakness in an organisation's people, process or technology infrastructure
- Using humans to infiltrate organisations is a common factor in most current cybercrime attacks
- Effective processes together with a risk management approach are crucial
- Organisations benefit from a multi-layered risk management strategy – 'defence in depth'
- The agility to know, control and adapt to new cyber threats will differentiate the strong from the weak
- Cyber resilience plans are essential – expect cyber disruption and prepare to deal with it while continuing to operate your business
- ANZ works with our clients to help keep them safe

CYBERCRIME INNOVATION

Cybercrime continues to threaten the Australian business landscape, with cybercrime expertise improving and adapting to target specific businesses. The ACSC (Australian Cybersecurity Centre) reports the changing environment has seen more diverse and innovative attempts to compromise government and private sector networks, increasing numbers of DDoS incidents, deliberate targeting, and changes in the frequency, scale, sophistication and severity of cyber incidents.[1]

Cybercriminals are increasingly sophisticated in their execution and can be equally opportunistic in who they target – from individuals through to large multi-national corporations, no one is immune from being attacked. This sophistication reflects the innovative methods used and speed of the execution. Cybercriminals innovate, make decisions and execute faster than many organisations are equipped to deal with. Moreover, cybercrime is now a business in every respect, with services that mirror those of multi-national organisations including customer support and technical helplines to ensure their criminal products and services work as intended.

In order to protect your business, you must understand this changing landscape and adapt.

Any modern corporate finance function is comprised of three main elements – people, process and technology. Cybercriminals look for and exploit any weakness in one or more of these elements to infiltrate the business to gain access to either information or syphon money, often millions of dollars at a time, into their international network.

CYBERCRIMINALS INNOVATE, MAKE DECISIONS AND EXECUTE FASTER THAN MANY ORGANISATIONS ARE EQUIPPED TO DEAL WITH.

CYBERCRIME IN ACTION

In March 2017, a Lithuanian man was arrested for duping two unnamed multinational internet companies via an email phishing attack. Google and Facebook later confirmed they were the two companies that fell victim to the scam costing them $100 million USD. He allegedly posed as a manufacturer in Asia and defrauded the companies from 2013 until 2015, stashing the money in bank accounts across Eastern Europe.

The emails were sent from accounts designed to look like they had come from an Asian-based manufacturer, but they did not. He used methods such as forging invoices, corporate stamps and email addresses to impersonate this Asian-based manufacturer with whom Facebook and Google regularly did business with.

This attack highlights how sophisticated cyber enabled fraud scams can fool even the biggest technology companies.[2]

On Friday, 12 May, 2017, the world was alarmed to discover that cybercrime had achieved a new record. In a widespread ransomware attack that hit organizations in more than 100 countries within the span of 48 hours, the operators of malware known as 'WannaCry' were believed to have caused the biggest attack of its kind ever recorded. Hospitals, rail systems, telecommunications and courier services were all impacted by WannaCry but many other organisations and individuals were affected as well.

According to an IBM report, ransomware was the most prevalent online threat in 2016. IBM researchers tracking spam trends noted that the rise in ransomware spam in 2016 reached an exorbitant 6,000 percent, going from 0.6 percent of spam emails in 2015 to an average of 40 percent of email spam in 2016. The situation is only worsening in 2017. The FBI estimated that ransomware is on pace to become a $1 billion source of income for cybercriminals by the end of 2016, a number that is expected to continue to rise in 2017.[3]

[1] https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf
[2] https://www.scmagazineuk.com/facebook-and-google-confirm-falling-victim-to-77m-phishing-scam/article/663207/
[3] https://securityintelligence.com/wannacry-ransomware-spreads-across-the-globe-makes-organizations-wanna-cry-about-microsoft-vulnerability/

Sub-task 5:

- *The user also accessed a file called "hiddenmessage2.txt"*
- *What is the contents of this file? Include it in your report*
  I viewed the TCP stream of this file, and noticed that instead of being plain text it was encoded data and when viewed as hex it had the same file signature as a jpg image. So I copied and saved the hex data with HxD as I have for other images, and discovered that the text file was actually this image.

Sub-task 6:

- *The user accessed an image called "atm-image.jpg"*
- *Identify what is different about this traffic and include everything in your report*
  Initial steps are same as the above steps like following TCP stream and after that we will get 3 images from following the procedure .


ANZ
ATM
ANZ
ATM
ANZ


shutterstock.com • 567329461

So the thing that is different about this traffic is that a single GET request performed by the user downloaded two images

Sub-task 7:

- *The network traffic shows that the user accessed the image "broken.png"*
- *Extract and include the image in your report.*
  First I filtered the packet capture for http traffic and looked through the remaining packets for the GET request that downloaded the image. I then right clicked the image and followed its TCP stream. In the TCP stream I saw what looked like image data. In order to view the data in hex format, I changed the view to „raw", and then searched the hex data for a jpeg"s file signature. After finding the file signature "89 50 4e 47 0d 0a 1a 0a" I copied everything after that point to the end and then copied into the hex editor HxD and saved it as a png image. The image as follow:

Sub-task 8:

- *The user accessed one more document called securepdf.pdf*
- *Access this document include an image of the pdf in your report. Detail the steps to access it.*

After investigating TCP stream for securepdf.pdf I discovered the following thing: The data there was not for a PDF. The bottom of the file contained the hidden message: Password is "secure" It contained the file signature for a zip file, meaning that the user downloaded was actually a zip file.so i copied that hex data and rendered it to zip file and i opened the zip file and it had the rawpdf.pdf and it was password secured and entered the "secure"

YOUR GUIDE TO ANZ INTERNET BANKING

ANZ

TABLE OF CONTENTS