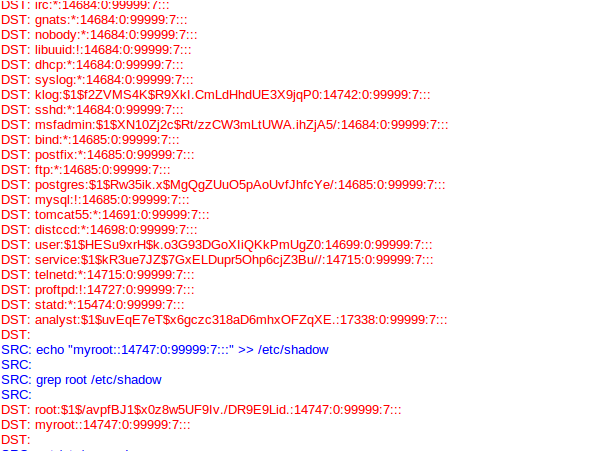
Mateusz Łąpieś ([mateusz.lapies@student.pk.edu.pl](mailto:mateusz.lapies@student.pk.edu.pl))

## Sprawozdanie – lab2

1. **What kind of transactions occurred between the client and the server in this attack?  
   Obraz zawierający tekst

   Opis wygenerowany automatycznie  
   Obraz zawierający tekst

   Opis wygenerowany automatycznie  
     
   Obraz zawierający tekst

   Opis wygenerowany automatycznie  
   **
2. **What did you observe? What do the text colors red and blue indicate?**Można zaobserwować te same komendy, które były widoczne w Transkrypcie, kolor czerwony reprezentuje atakującego, niebieskie serwer.  
   **The attacker issues the whoami command on the target. What does this show about the attacker role on the target computer?**Odpowiedź potwierdza, że atakujący otrzymał rolę roota (administratora).  
   **Scroll through the TCP stream. What kind of data has the threat actor been reading?**nazwa hosta  
   interfejsy sieciowe  
   użytkownicy i uprawnienia
3. **What are the source and destination IP addresses and port numbers for the FTP traffic?**Source: 192.168.0.11 Destination: 209.165.200.235 Port: 52776/21  
   **What are the user credentials to access the FTP site?**User: analyst  
   Pass: cyberops  
   **What are the different types of files? Look at the MIME Type section of the screen.**Dla 11.06.2020 był to jeden plik o typie text/plain.  
   **What is the MIME type, source and destination IP address associated with the transfer of the FTP data? When did this transfer occur?**Type: text/plain, Source: 192.168.0.11, Destination: 209.165.200.235.  
   June 11th 2020, 03:53:09.088  
   **What is the text content of the file that was transferred using FTP?**  
   **  
   With all the information has gathered so far, what is your recommendation for stopping further unauthorized access?**Należy ograniczyć dostęp dla Destination IP do sieci / maszyny. Ograniczyć dostęp użytkowników do FTP. Zabezpieczyć połączenie przechodząc z FTP na FTPs.