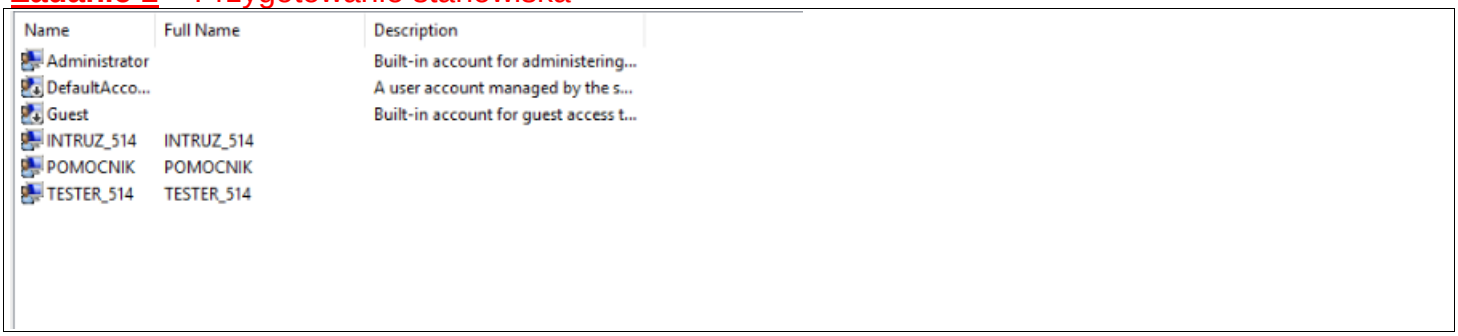
Temat 03.4 – Wybrane metody enumeracji

Wykonał(a): Bartosz Miazga
Stanowisko: 14

Zadanie 1 – Przygotowanie stanowiska

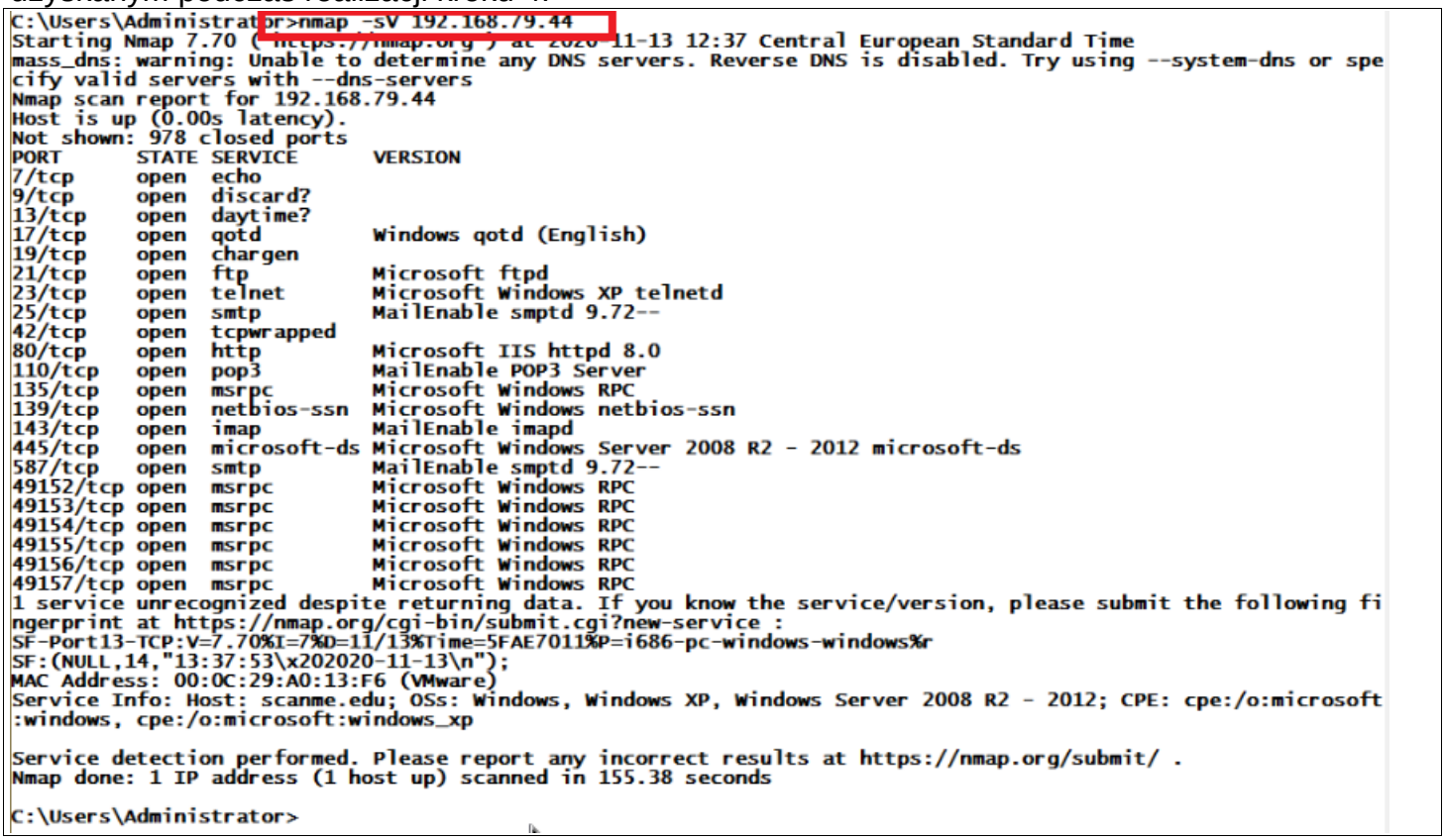


Name	Full Name	Description
Administrator		Built-in account for administering...
DefaultAcco...		A user account managed by the s...
Guest		Built-in account for guest access t...
INTRUZ_514	INTRUZ_514	
POMOCNIK	POMOCNIK	
TESTER_514	TESTER_514	

1. (poniżej) Obraz okna konsoli zarządzania komputerem (*Computer Management*) prezentującego listę kont użytkowników – *po zrealizowania zadania 1*

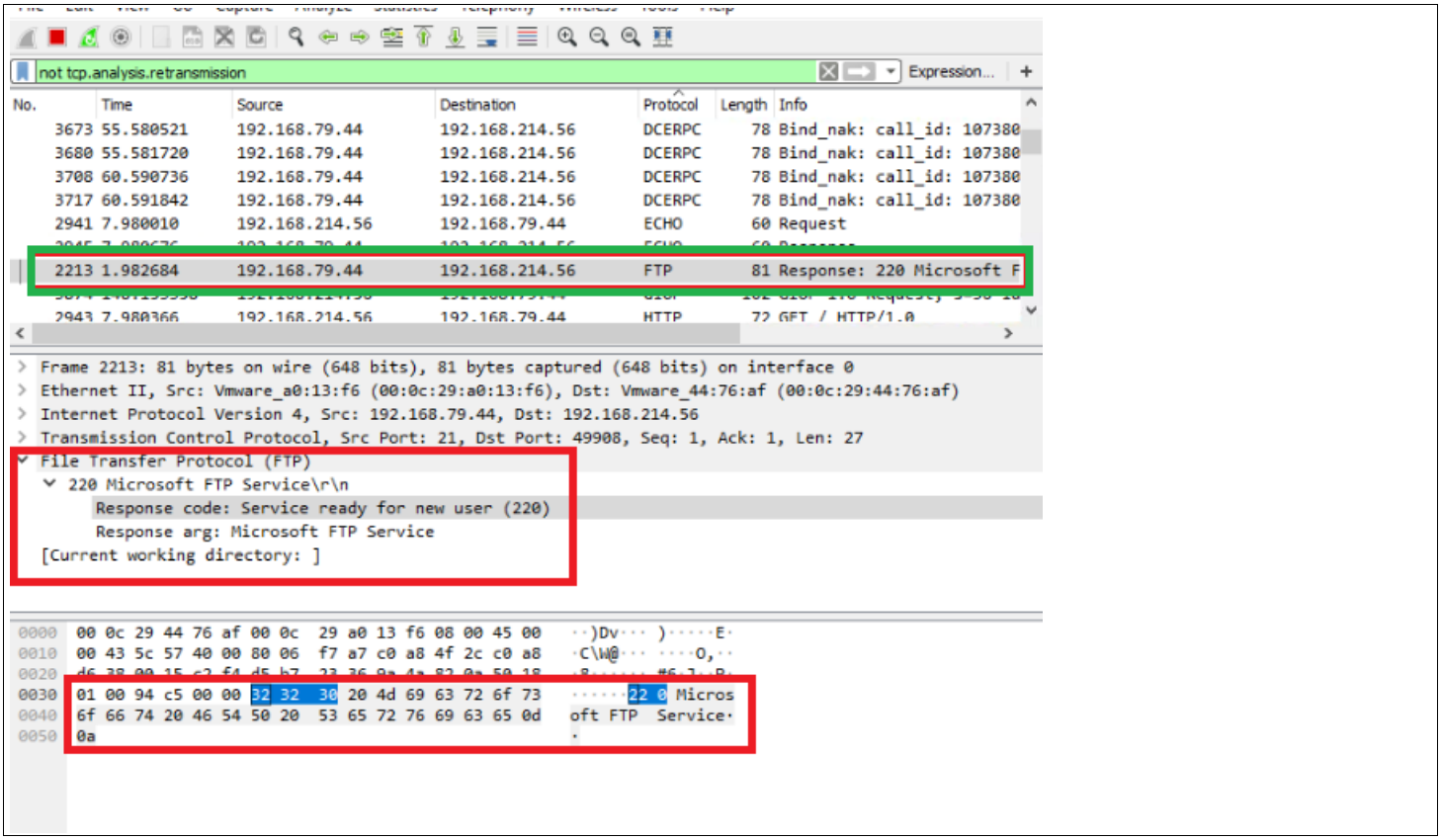
Zadanie 2 – Pozyskiwanie banerów aplikacji za pomocą programu ***nmap***

2.1 (poniżej) Obraz okna wiersza poleceń z zaznaczoną linią polecenia i raportem programu *nmap* uzyskanym podczas realizacji kroku 4.

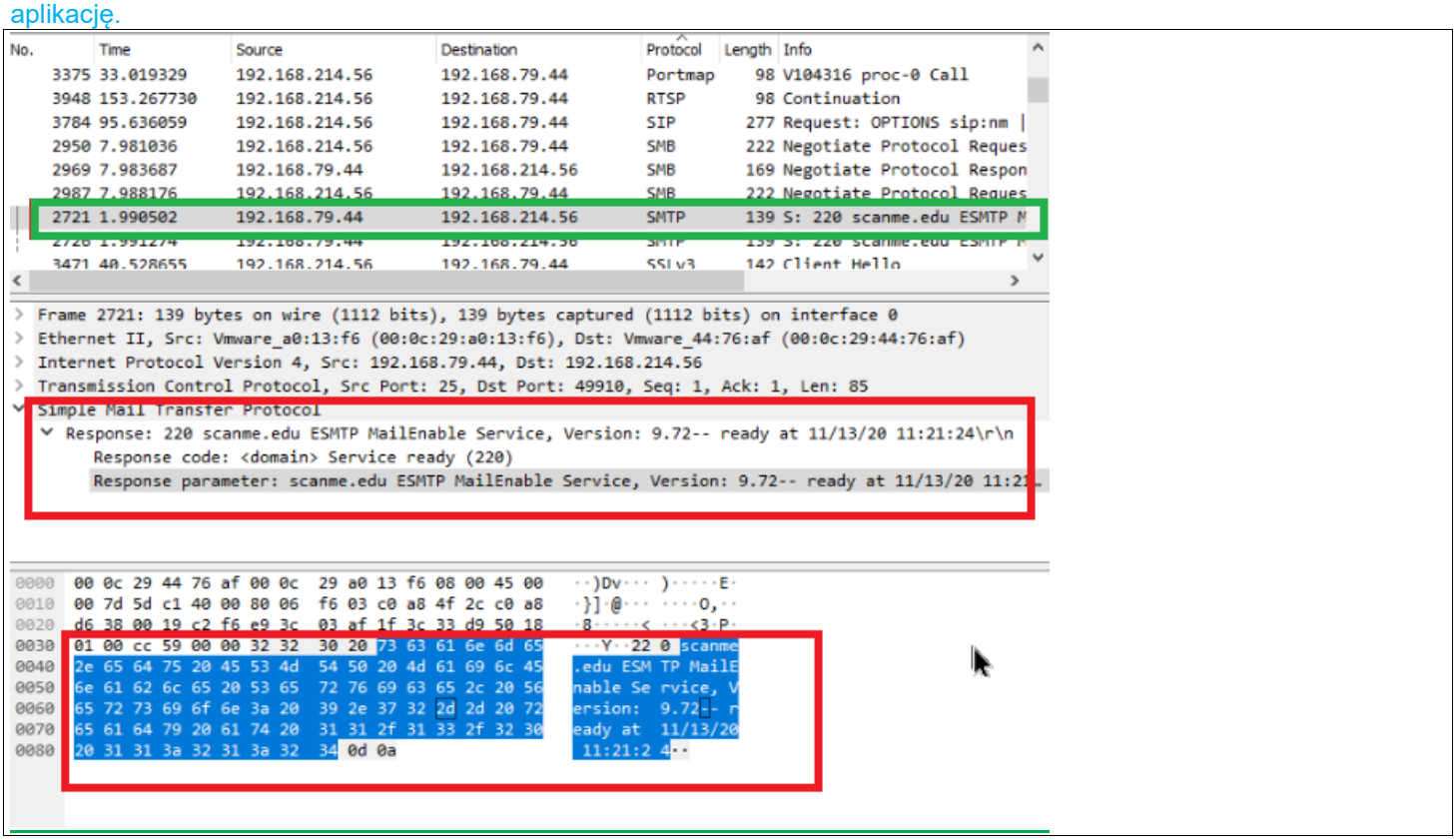


```
C:\Users\Administrator>nmap -sV 192.168.79.44
Starting Nmap 7.70 ( https://nmap.org ) at 2020-11-13 12:37 Central European Standard Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or spe
cify valid servers with --dns-servers
Nmap scan report for 192.168.79.44
Host is up (0.00s latency).
Not shown: 978 closed ports
PORT      STATE SERVICE      VERSION
7/tcp     open  echo
9/tcp     open  discard?
13/tcp    open  daytime?
17/tcp    open  qotd         Windows qotd (English)
19/tcp    open  chargen
21/tcp    open  ftp          Microsoft ftpd
23/tcp    open  telnet       Microsoft Windows XP telnetd
25/tcp    open  smtp         MailEnable smptd 9.72--
42/tcp    open  tcpwrapped
80/tcp    open  http         Microsoft IIS httpd 8.0
110/tcp   open  pop3         MailEnable POP3 Server
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
143/tcp   open  imap         MailEnable imapd
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
587/tcp   open  smtp         MailEnable smptd 9.72--
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the following fi
ngerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port13-TCP:V=7.70%I=7%D=11/13%Time=5FAE7011%P=i686-pc-windows-windows%r
SF:(NULL,14,"13:37:53\x202020-11-13\n");
MAC Address: 00:0C:29:A0:13:F6 (VMware)
Service Info: Host: scanme.edu; OSs: Windows, Windows XP, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft
:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 155.38 seconds

C:\Users\Administrator>
```

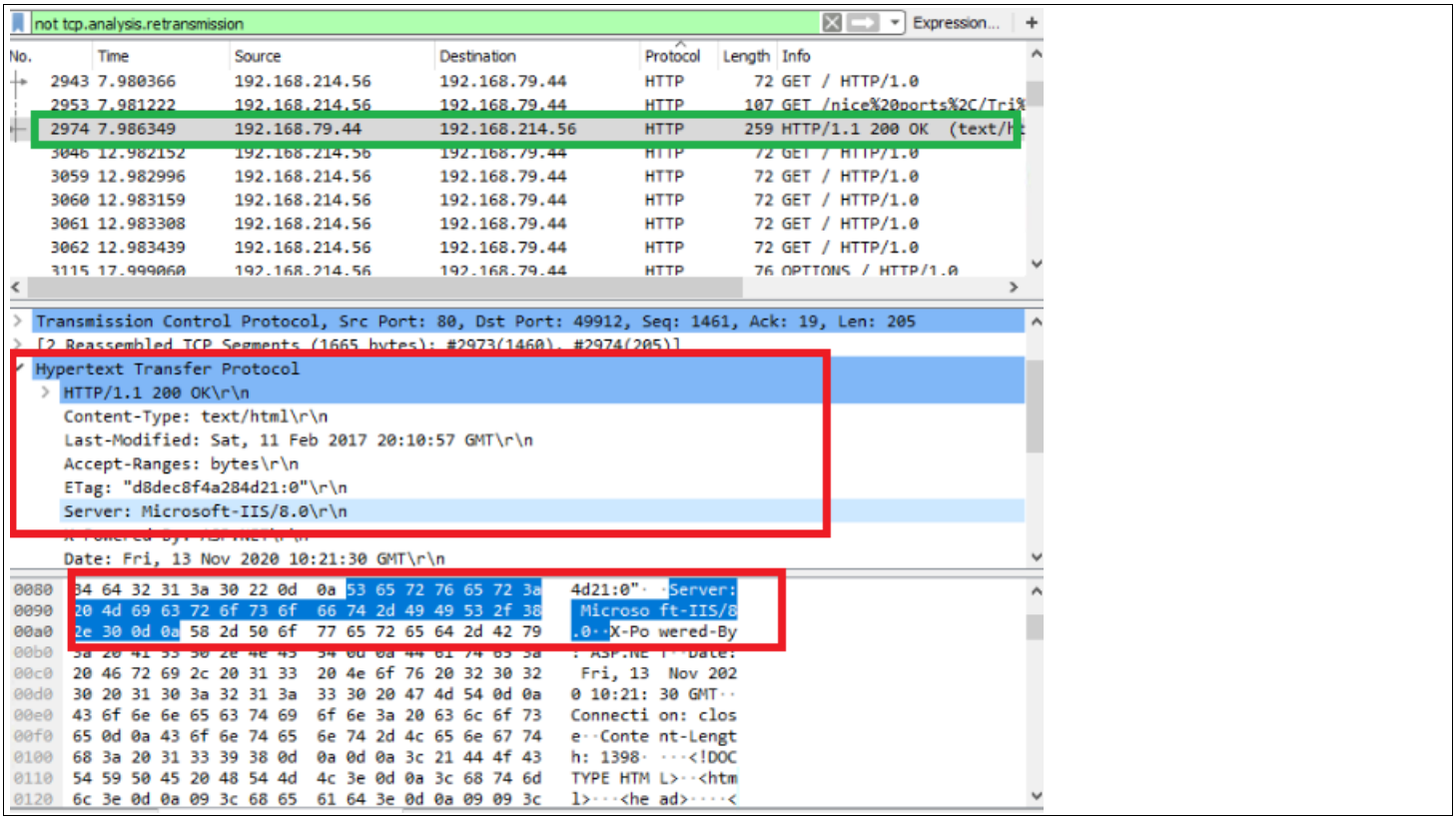
2.2 (poniżej) Obraz okna sniffera uzyskany podczas badania przeprowadzonego z wykorzystaniem programu *nmap* w kroku 4. Kolorem zielonym zaznaczono w panelu listy pakietów (*Packet List*), pakiet zawierający dane enumeracyjne procesu usługi dostępnej na porcie 21. Kolorem czerwonym zaznaczono w panelu listy pakietów i panelu szczegółów wybranego pakietu (*Packet Details lub Packet Bytes*), dane pozwalające zidentyfikować uruchomioną aplikację.



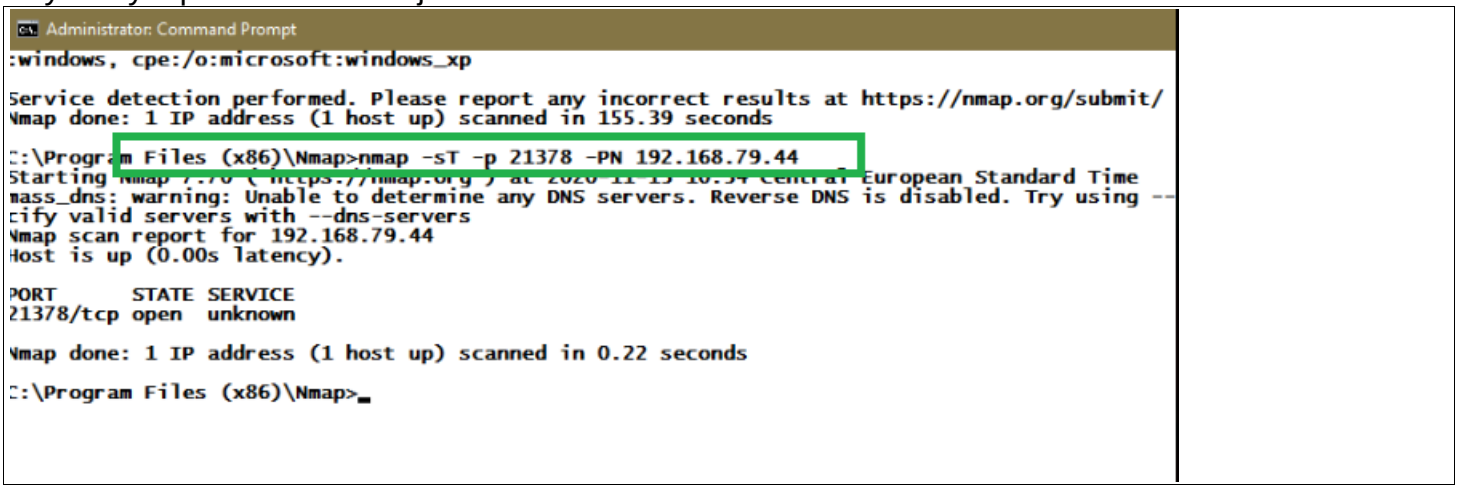
2.3 (poniżej) Obraz okna sniffera uzyskany podczas badania przeprowadzonego z wykorzystaniem programu *nmap* w kroku 4. Kolorem zielonym zaznaczono w panelu listy pakietów (*Packet List*), pakiet zawierający dane enumeracyjne procesu usługi dostępnej na porcie 25. Kolorem czerwonym zaznaczono w panelu listy pakietów i panelu szczegółów wybranego pakietu (*Packet Details lub Packet Bytes*), dane pozwalające zidentyfikować uruchomioną aplikację.



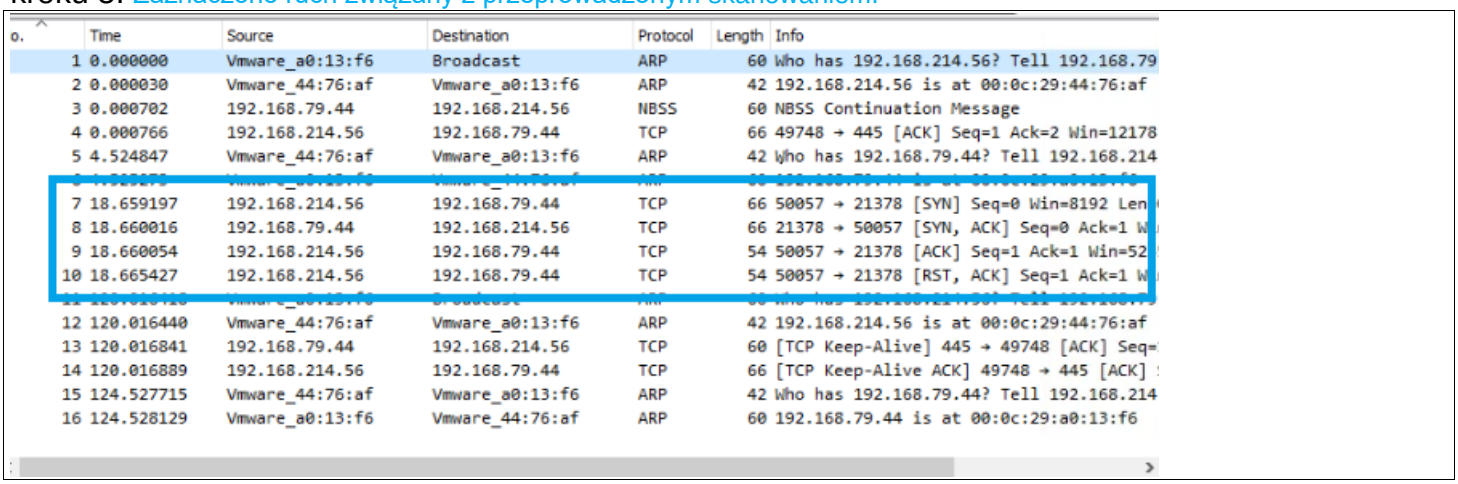
2.4 (poniżej) Obraz okna sniffera uzyskany podczas badania przeprowadzonego z wykorzystaniem programu *nmap* w kroku 4. Kolorem zielonym zaznaczono w panelu listy pakietów (*Packet List*), pakiet zawierający dane enumeracyjne procesu usługi dostępnej na porcie 80. Kolorem czerwonym zaznaczono w panelu szczegółów wybranego pakietu (*Packet Details lub Packet Bytes*), dane pozwalające zidentyfikować uruchomioną aplikację.



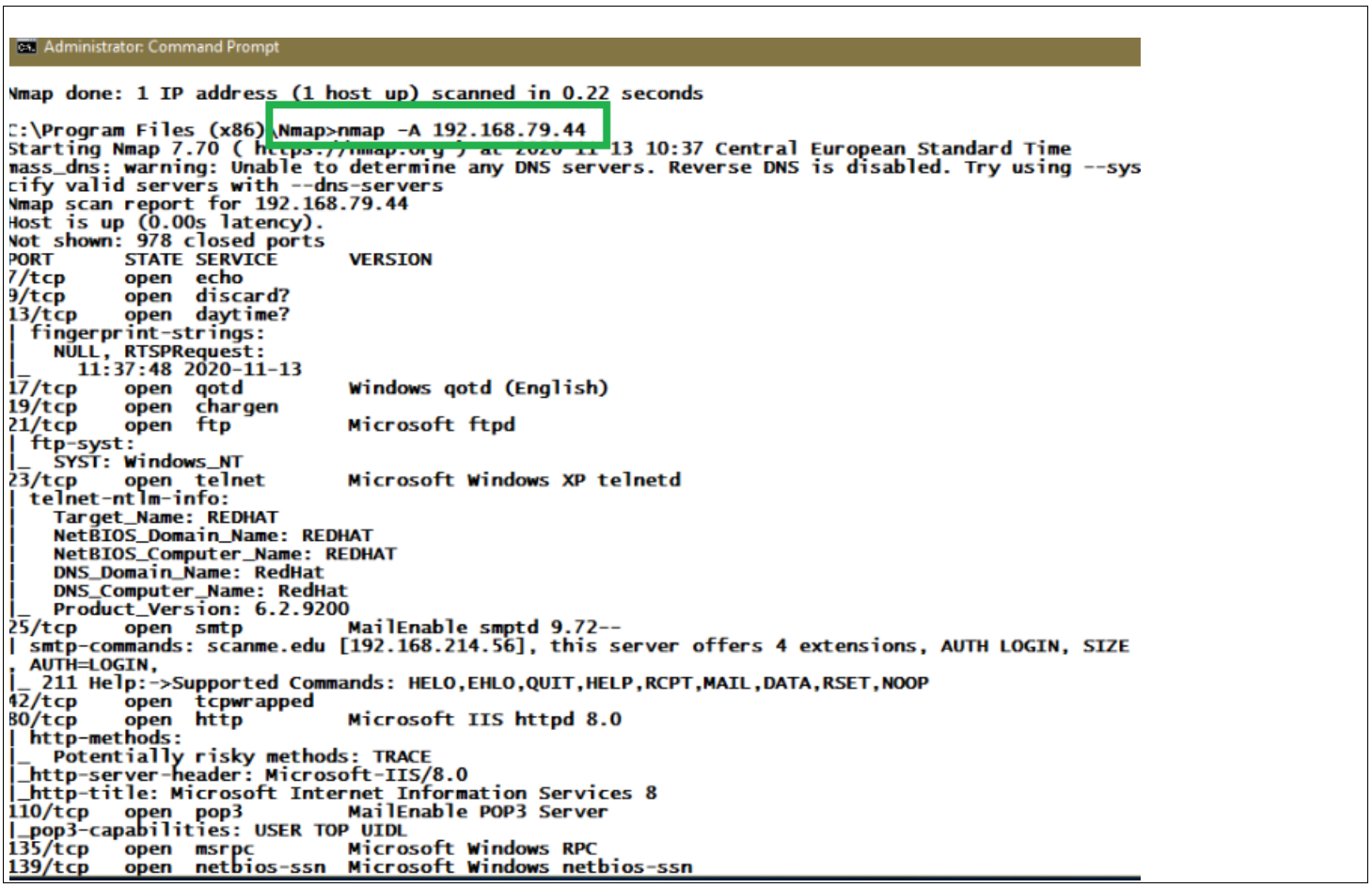
2.5a (poniżej) Obraz okna wiersza poleceń z zaznaczoną linią polecenia i raportem programu *nmap* uzyskanym podczas realizacji kroku 5.

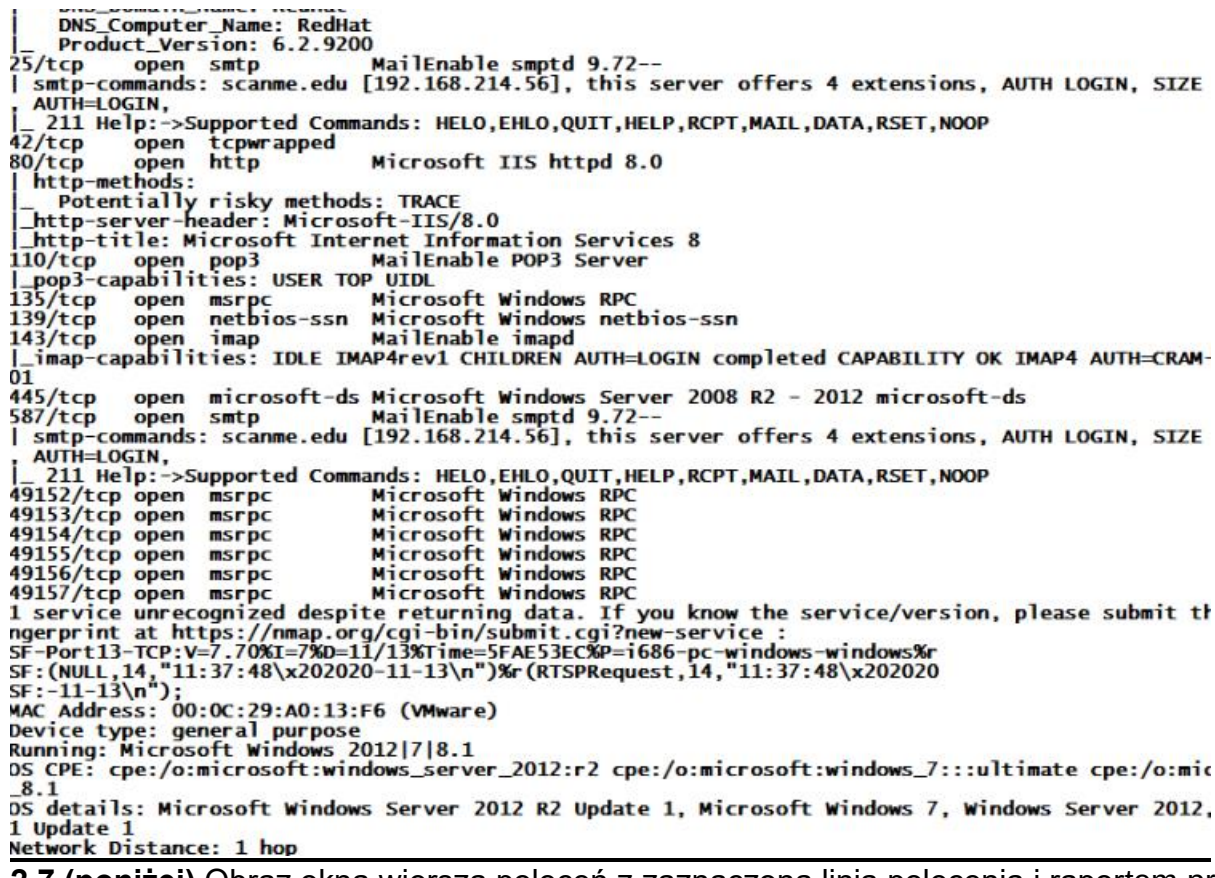


2.5b (poniżej) Obraz okna sniffera uzyskany podczas badania przeprowadzonego podczas realizacji kroku 5. Zaznaczono ruch związany z przeprowadzonym skanowaniem.



2.6 (poniżej) Obraz okna/okien wiersza poleceń z zaznaczoną linią polecenia i raportem programu *nmap* uzyskanym podczas realizacji kroku 6.





2.7 (poniżej) Obraz okna wiersza poleceń z zaznaczoną linią polecenia i raportem programu *nmap* uzyskanym podczas realizacji kroku 7.

```
C:\Users\Administrator>nmap -A 192.168.79.44 -p 21378
Starting Nmap 7.70 ( https://nmap.org ) at 2020-11-13 12:52 Central European Standard Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or spe
cify valid servers with --dns-servers
Nmap scan report for 192.168.79.44
Host is up (0.00s latency).

PORT      STATE SERVICE VERSION
21378/tcp open  ftp     Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_04-08-17  08:15PM       <DIR>          aspnet_client
| ftp-syst:
|_  SYST: Windows_NT
MAC Address: 00:0C:29:A0:13:F6 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2012|7|8.1
OS CPE: cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_7:::ultimate cpe:/o:microsoft:windows
_8.1
OS details: Microsoft Windows Server 2012 R2 Update 1, Microsoft Windows 7, Windows Server 2012, or Windows 8.
1 Update 1
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT     ADDRESS
1   0.00 ms 192.168.79.44

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.42 seconds

C:\Users\Administrator>
```


2.8 Opis zaobserwowanych efektów oraz wnioski dotyczące zadania:

m.in. dokładny opis informacji uzyskanych za pomocą banerów oraz charakterystyka ruchu sieciowego obserwowanego podczas badania.

W wyniku użycia programu nmap ,dzięki pozyskanym banerom możemy uzyskać informacje o uruchomionych usługach oraz ich wersjach na maszynie poddanej skanowaniu, dla wskazanych portów udało się zauważyć następujące usługi:

1.port 21 - ftp
2.port 25 - SMTP
3.port 80 - http z zainstalowanym programem IIS

W kroku 4. port 21378 nie zostaje uwzględniony w raporcie programu nmap
W kroku 5. nmap nie pokazuje żadnej usługi dla portu 21378 mimo , że jest on otwarty.
W kroku 6. dostajemy bardziej szczegółowe informacje w raporcie niż w kroku 4. jednakże port 21378 również nie zostaje uwzględniony.
W kroku 7. w raporcie można zauważyć usługę ftp dla portu 21378 oraz informację "Anonymous ftp login allowed", użytkownik „anonimowy” ma ograniczone prawa dostępu do hosta archiwum, a także pewne ograniczenia operacyjne. Być może dlatego w poprzednich próbach nie otrzymywałem informacji o usłudze na danym porcie.

Zadanie 3 – Pozyskiwanie banerów aplikacji za pomocą programu *telnet*

3.1 (poniżej) Obraz okna wiersza poleceń z raportem programu *telnet* uzyskanym podczas realizacji kroku 3.

Wkleić obraz okna

3.2 (poniżej) Obraz okna sniffera uzyskany podczas badania przeprowadzonego w kroku 3. Kolorem zielonym zaznaczono w panelu listy pakietów (*Packet List*), pakiet zawierający dane enumeracyjne procesu usługi dostępnej na porcie 21. Kolorem czerwonym zaznaczono w panelu listy pakietów i panelu szczegółów wybranego pakietu (*Packet Details lub Packet Bytes*), dane pozwalające zidentyfikować uruchomioną aplikację.

Wkleić obraz okna

3.3 (poniżej) Obraz okna wiersza poleceń z raportem programu *telnet* uzyskanym podczas realizacji kroku 6.

Wkleić obraz okna

3.4 (poniżej) Obrazy okien sniffera uzyskane podczas badania przeprowadzonego w kroku 6. Kolorem zielonym zaznaczono w panelu listy pakietów (*Packet List*), pakiety zawierające dane enumeracyjne procesu usługi dostępnej na porcie 21378. Kolorem czerwonym zaznaczono w panelu szczegółów (*Packet Details lub Packet Bytes*), dane pozwalające zidentyfikować uruchomioną aplikację.

Wkleić obrazy okien

3.5 Opis zaobserwowanych efektów oraz wnioski dotyczące zadania:

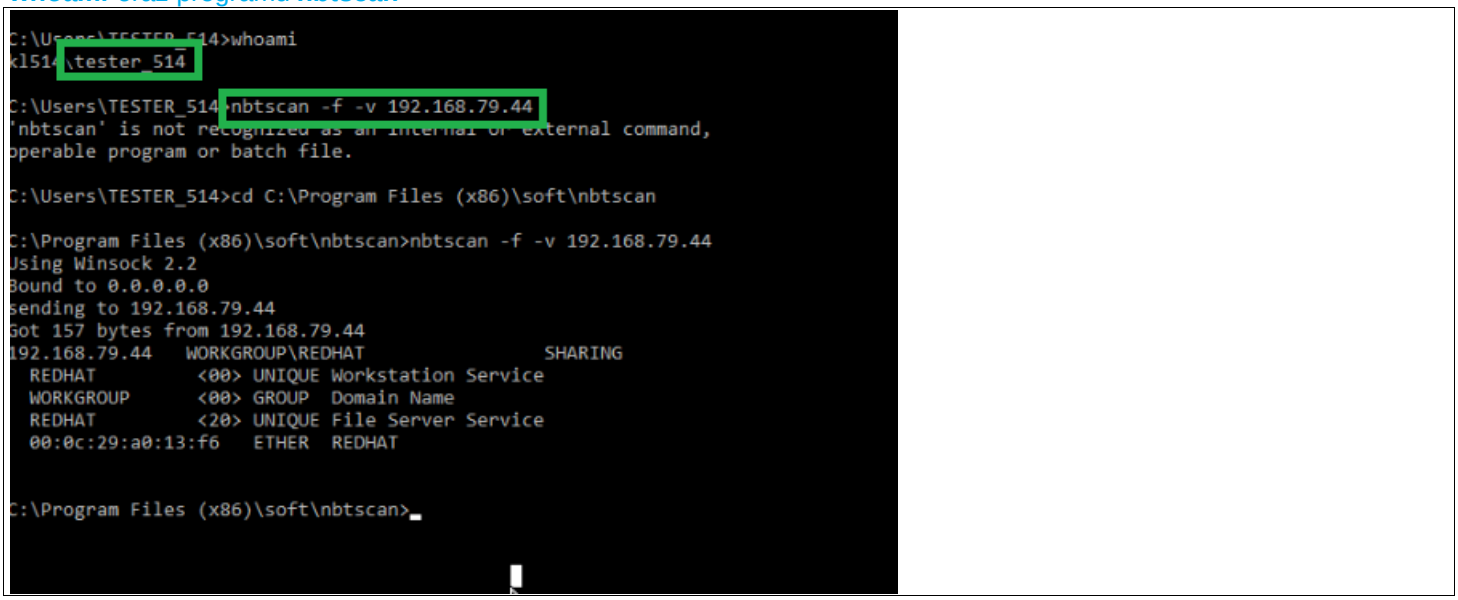
m.in. opisy określone w instrukcji kolorem zielonym, w tym dokładny opis informacji uzyskanych za pomocą banerów oraz charakterystyka ruchu sieciowego obserwowanego podczas badania.

.....

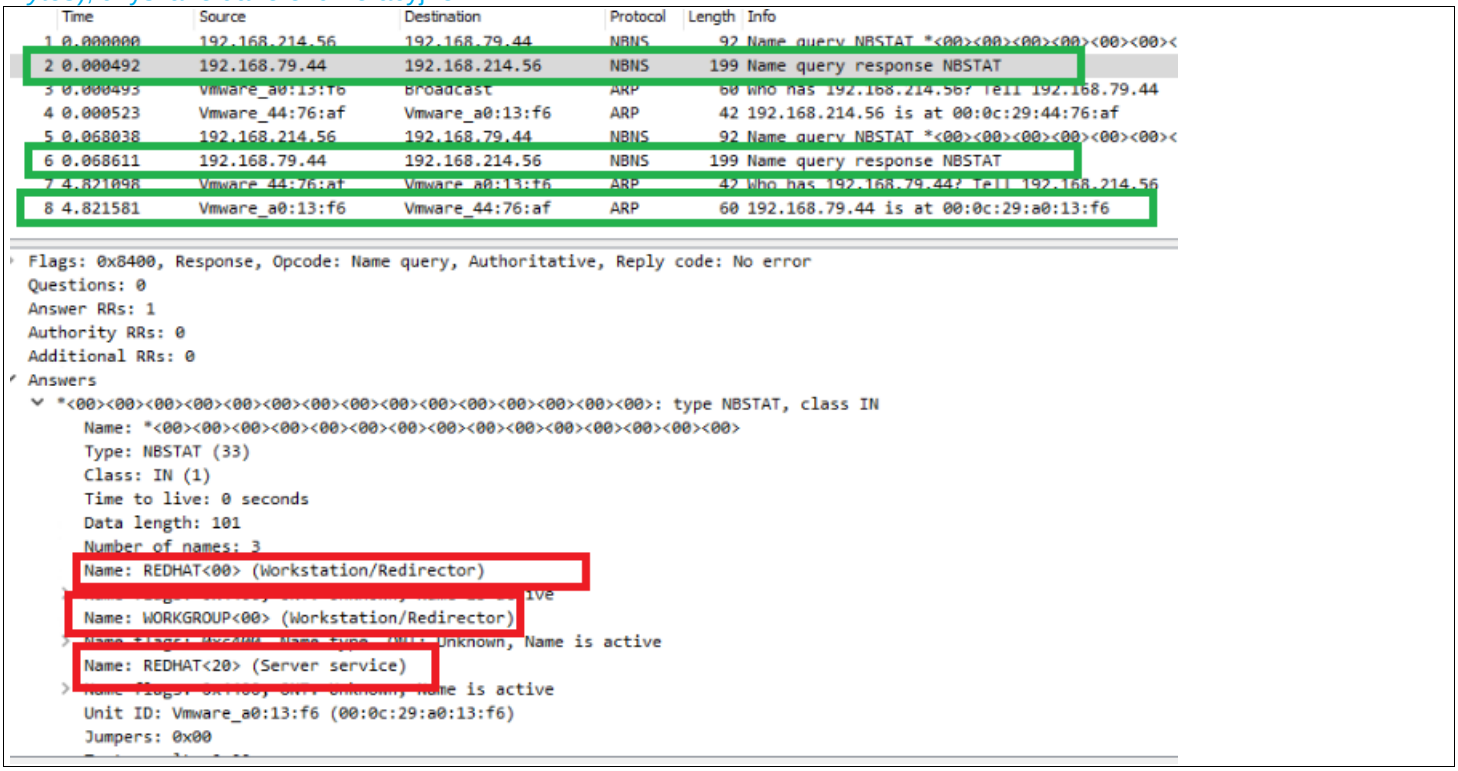
.....

Zadanie 4 – Enumeracja za pomocą programu *nbtscan*

4.1 (poniżej) Obraz okna prezentującego raporty uzyskane podczas realizacji kroków 4 oraz 5.
W zamieszczonym oknie powinny być widoczne i zaznaczone linie zawierające polecenia uruchomienia programu ***whoami*** oraz programu ***nbtscan***



4.2 (poniżej) Obraz okna sniffera uzyskany podczas badania przeprowadzonego z wykorzystaniem programu *nbtscan* w kroku 4. Kolorem zielonym zaznaczono w panelu listy pakietów (*Packet List*), pakiety zawierające dane enumeracyjne. Kolorem czerwonym zaznaczono w panelu szczegółów (*Packet Details lub Packet Bytes*), uzyskane dane enumeracyjne.



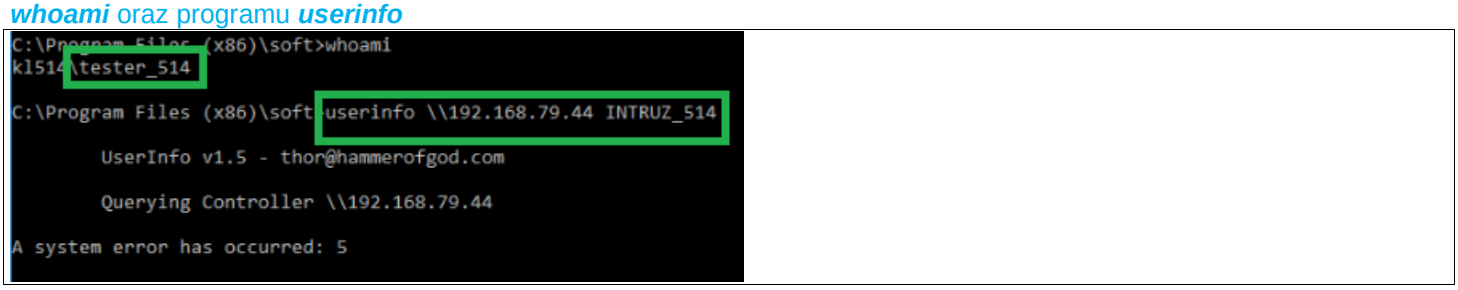
4.3 Opis zaobserwowanych efektów oraz wnioski dotyczące zadania:

m.in. opisy określone w instrukcji kolorem zielonym, w tym dokładny opis uzyskanych informacji oraz charakterystyka ruchu sieciowego obserwowanego podczas badania.

Pakiety służące do przekazania danych enumeracyjnych to pakiety UDP protokołu NBNS. **Dostęp do badanego komputera nie wymaga uwierzytelniania, nie są wymagane żadne uprawnienia**. Z raportów można uzyskać tablice nazw NetBIOS poszczególnych hostów w podsieci oraz można zidentyfikować aktywne hosty w podsieci poprzez skanowanie ARP. Do uzyskania informacji został wykorzystany protokół NBNS(NetBIOS) oraz ARP – skanowanie podsieci. Aby badany przypadek enumeracji był skuteczny należy wykorzystać pustą sesję, która zawiązuje się na koncie anonimowym bez hasła z ukrytym zasobem IPC$. Po utworzeniu takiej anonimowej sesji tester będzie mógł zidentyfikować udostępnione zasoby i użytkowników na testowanym komputerze.

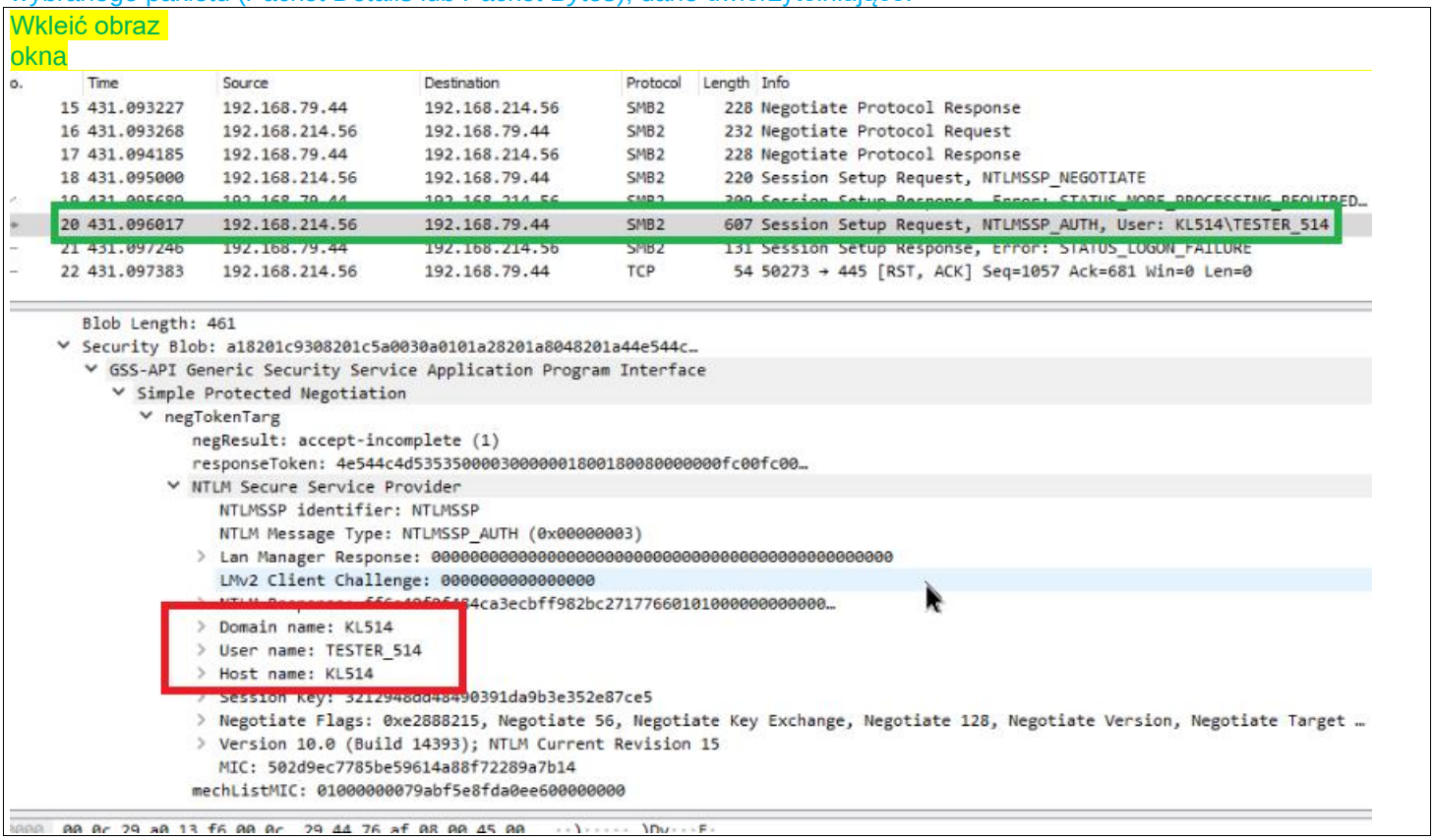
Zadanie 5 - Enumeracja za pomocą programu *userinfo*

5.1. (poniżej) Obraz okna prezentującego raporty uzyskane podczas realizacji kroków 4 i 5.
W zamieszczonym oknie powinny być widoczne i zaznaczone linie zawierające polecenia uruchomienia programu ***whoami*** oraz programu ***userinfo***

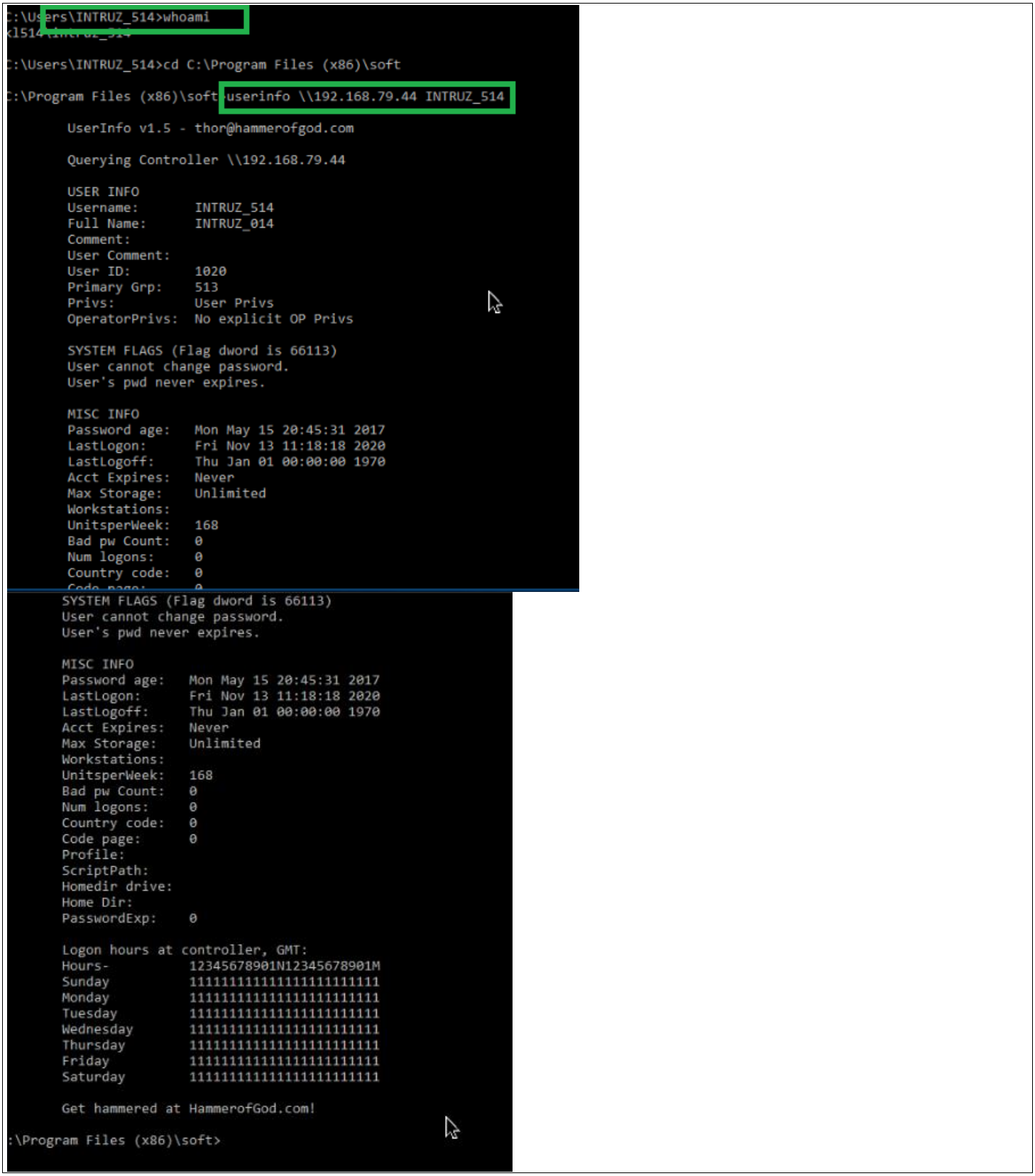


5.2 (poniżej) Obraz okna sniffera uzyskany podczas badania przeprowadzonego z wykorzystaniem programu *userinfo* w kroku 5. Kolorem zielonym zaznaczono w panelu listy pakietów (*Packet List*), pakiety związane z procesem uwierzytelnienia. Kolorem czerwonym zaznaczono w panelu listy pakietów i panelu szczegółów wybranego pakietu (*Packet Details lub Packet Bytes*), dane uwierzytelniające.

Wkleić obraz okna



5.3. (poniżej) Obrazy okien prezentujących raporty uzyskane podczas realizacji kroków 4 i 10.
W każdym zamieszczonym oknie powinny być widoczne i zaznaczone linie zawierające polecenia uruchomienia *programu* ***whoami*** *oraz programu* ***userinfo***

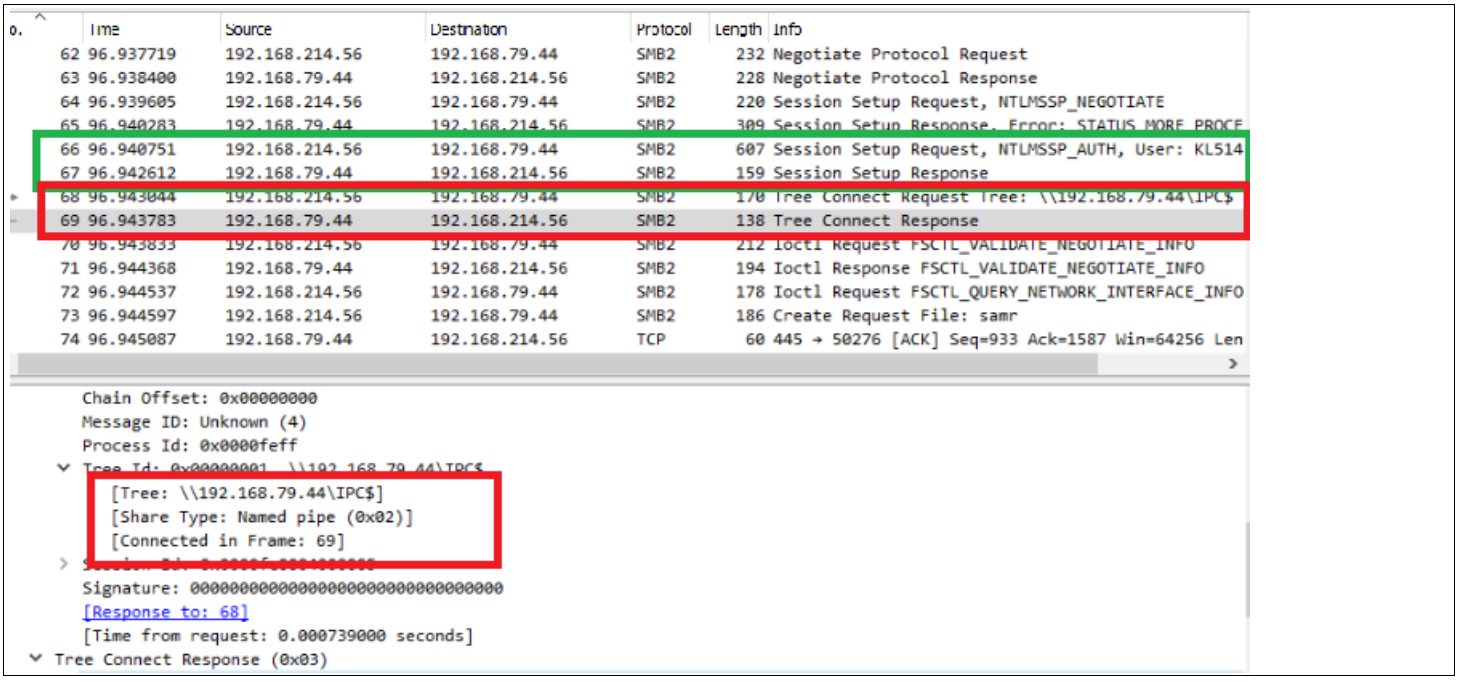


<u>Oraz dla Guest:</u>

```
:\Program Files (x86)\soft>userinfo \\192.168.79.44 GUEST

      UserInfo v1.5 - thor@hammerofgod.com

      Querying Controller \\192.168.79.44

      USER INFO
      Username:       Guest
      Full Name:
      Comment:        Built-in account for guest access to the computer/domain
      User Comment:
      User ID:        501
      Primary Grp:    513
      Privs:          Guest Privs
      OperatorPrivs:  No explicit OP Privs

      SYSTEM FLAGS (Flag dword is 66147)
      This account is disabled.
      User cannot change password.
      User's pwd never expires.

      MISC INFO
      Password age:   Fri Nov 13 10:19:55 2020
      LastLogon:      Thu Jan 01 00:00:00 1970
      LastLogoff:     Thu Jan 01 00:00:00 1970
      Acct Expires:   Never
      Max Storage:    Unlimited
      Workstations:
      UnitsperWeek:   168
      Bad pw Count:   0
      Num logons:     0
      Country code:   0
      Code page:      0
      Profile:
      ScriptPath:
      Homedir drive:
      Home Dir:
      PasswordExp:    0
```

```
      MISC INFO
      Password age:   Fri Nov 13 10:19:55 2020
      LastLogon:      Thu Jan 01 00:00:00 1970
      LastLogoff:     Thu Jan 01 00:00:00 1970
      Acct Expires:   Never
      Max Storage:    Unlimited
      Workstations:
      UnitsperWeek:   168
      Bad pw Count:   0
      Num logons:     0
      Country code:   0
      Code page:      0
      Profile:
      ScriptPath:
      Homedir drive:
      Home Dir:
      PasswordExp:    0

      Logon hours at controller, GMT:
      Hours-          12345678901N12345678901M
      Sunday          111111111111111111111111
      Monday          111111111111111111111111
      Tuesday         111111111111111111111111
      Wednesday       111111111111111111111111
      Thursday        111111111111111111111111
      Friday          111111111111111111111111
      Saturday        111111111111111111111111

      Get hammered at HammerofGod.com!

\Program Files (x86)\soft>_
```

5.4. (poniżej) Obraz okna sniffera uzyskany podczas badania przeprowadzonego z wykorzystaniem programu *userinfo* w kroku 10 dla konta *guest*. Kolorem zielonym zaznaczono w panelu listy pakietów (*Packet List*), pakiety związane z procesem uwierzytelnienia. Kolorem czerwonym zaznaczono w panelu listy pakietów, pakiet podłączenia do udziału umożliwiającego enumerację i panelu szczegółów (*Packet Details*), dane uwierzytelniające wykorzystywane podczas tego podłączenia oraz ścieżkę dostępu do tego udziału.



5.5 Opis zaobserwowanych efektów oraz wnioski dotyczące zadania:

m.in. opisy określone w instrukcji kolorem zielonym, w tym dokładny opis uzyskanych informacji oraz charakterystyka ruchu sieciowego obserwowanego podczas badania.

Z otrzymanych raportów można uzyskać wiele informacji, między innymi ID użytkownika , główna grupa, flagi systemowe, informacje dotyczące hasła, w tym wiek hasła. Do otrzymania takich informacji został wykorzystany protokół SMB2. Aby przypadek enumeracji był skuteczny konieczne jest posiadanie konta użytkownika znajdującego się na enumerowanym komputerze (INTRUZ ma odpowiednik w systemie enumerowanym).

Zadanie 6– Enumeracja za pomocą programu *enum*

6.1. (poniżej) Obrazy okien prezentujących raporty uzyskane podczas kolejnych realizacji kroku 3.

Każdy cykl enumeracji (opisany w kroku 3) należy przedstawić w oddzielnym, pojedynczym oknie. W każdym zamieszczonym oknie powinny być widoczne i zaznaczone linie zawierające polecenia uruchomienia programu *whoami* oraz dwa uruchomienia programu *enum*.

Wkleić obrazy okien

6.2. (poniżej) Obrazy okien sniffera uzyskane podczas badania przeprowadzonego z wykorzystaniem programu *enum* w jednym z cykli w kroku 3. Kolorem zielonym zaznaczono w panelu listy pakietów (*Packet List*), pakiety związane z procesem uwierzytelnienia. Kolorem czerwonym zaznaczono w panelu listy pakietów, pakiet podłączenia do udziału umożliwiającego enumerację i panelu szczegółów (*Packet Details*), dane uwierzytelniające wykorzystywane podczas tego podłączenia oraz ścieżkę dostępu do tego udziału.

Wkleić obraz okna

6.3 Opis zaobserwowanych efektów oraz wnioski dotyczące zadania:

m.in. opisy określone w instrukcji kolorem zielonym, w tym dokładny opis uzyskanych informacji oraz charakterystyka ruchu sieciowego obserwowanego podczas badania.

.....

.....

Zadanie 7 - Enumeracja za pomocą programów ***user2sid*** oraz ***sid2user***

7.1a. (poniżej) Obraz okna prezentującego raporty uzyskane podczas realizacji kroków 4 oraz 5.

W zamieszczonym oknie powinny być widoczne i zaznaczone linie zawierające polecenia uruchomienia programu ***whoami*** oraz programu ***user2sid***

```
C:\Program Files (x86)\soft\snmpwalk>whoami
kl514\tester_514

C:\Program Files (x86)\soft\snmpwalk>cd C:\Program Files (x86)\soft\win_sid

C:\Program Files (x86)\soft\win_sid>user2sid \\192.168.79.44 REDHAT

LookupAccountName failed - no such account
```

7.1b. (poniżej) Obraz okna sniffera uzyskany podczas realizacji kroku 5. Kolorem zielonym zaznaczono w panelu listy pakietów (*Packet List*), pakiety związane z procesem uwierzytelnienia i panelu szczegółów (*Packet Details*), dane uwierzytelniające.

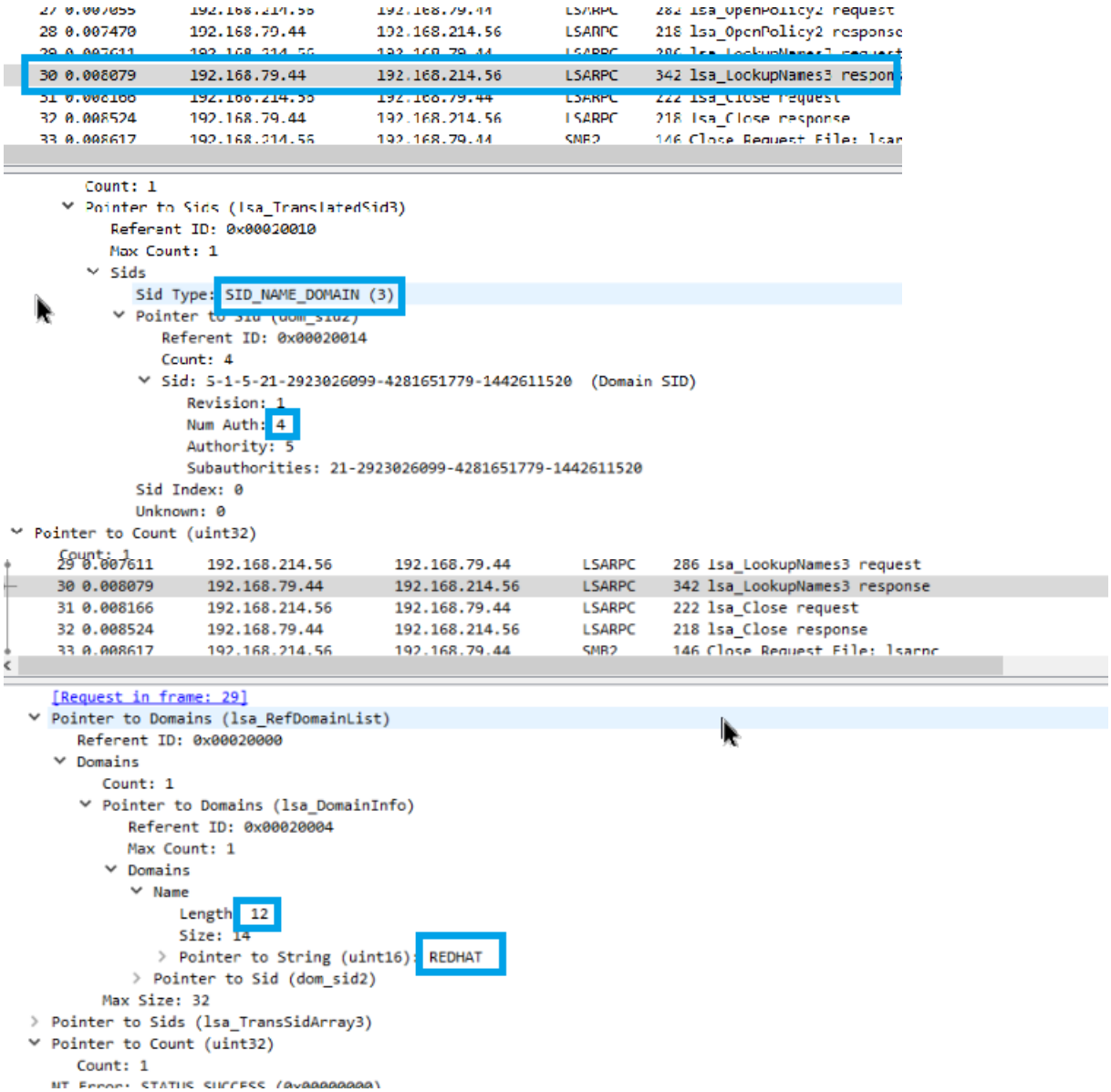
Wkleić obraz okna

7.2a. (poniżej) Obraz okna prezentującego raporty uzyskane podczas realizacji kroków 8 oraz 9. W zamieszczonym oknie powinny być widoczne i zaznaczone linie zawierające polecenia uruchomienia programu ***whoami*** oraz programu ***user2sid***

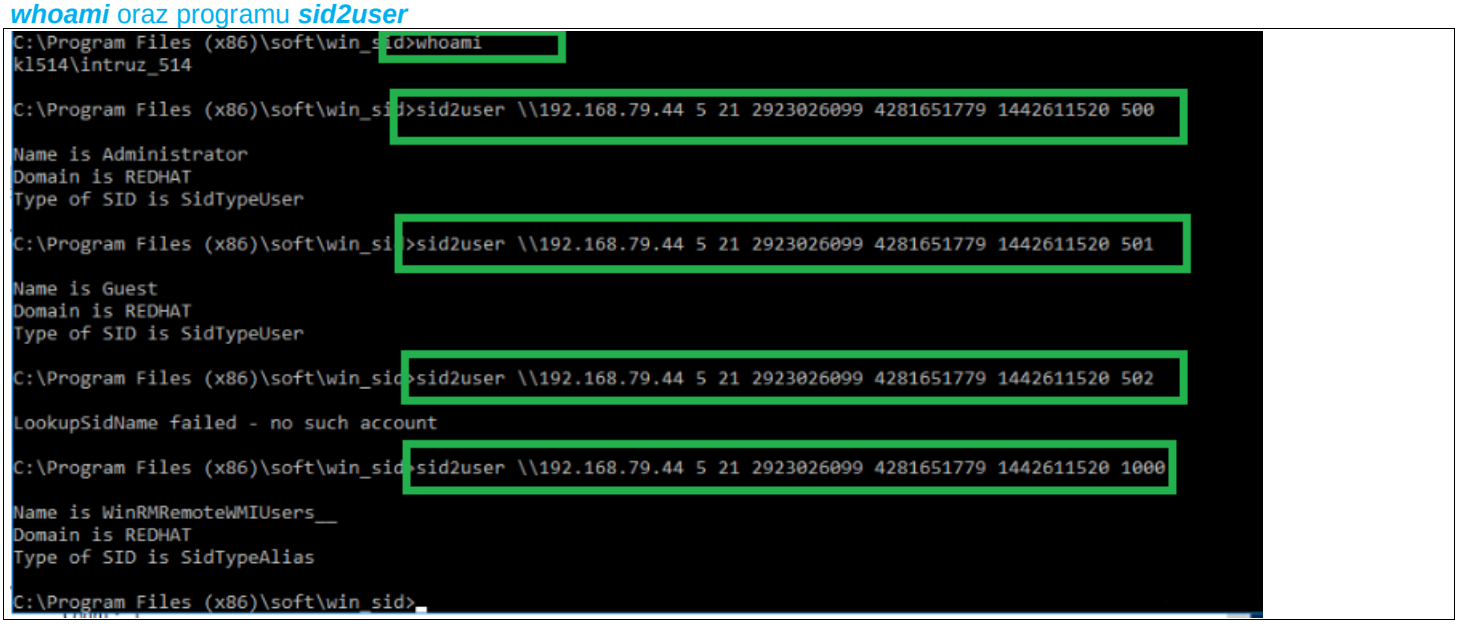
```
C:\Users\INTRUZ_514>whoami
kl514\intruz_514

C:\Users\INTRUZ_514>cd C:\Program Files (x86)\soft\win_sid

C:\Program Files (x86)\soft\win_sid>user2sid \\192.168.79.44 REDHAT

S-1-5-21-2923026099-4281651779-1442611520

Number of subauthorities is 4
Domain is REDHAT
Length of SID in memory is 24 bytes
Type of SID is SidTypeDomain
```

7.2b. (poniżej) Obraz okna sniffera uzyskany podczas realizacji kroku 9. Kolorem zielonym zaznaczono w panelu listy pakietów (*Packet List*), pakiety związane z procesem uwierzytelnienia, kolorem czerwonym zaznaczono pakiety podłączenia do udziału umożliwiającego enumerację a kolorem niebieskim pakiet zawierający zwracane dane enumeracyjne. W panelu szczegółów (*Packet Details*), kolorem niebieskim zaznaczono zwrócone dane enumeracyjne.

```
  9 0.001790    192.168.79.44    192.168.214.56   SMB2     228 Negotiate Protocol Response
 10 0.002490    192.168.214.56   192.168.79.44    SMB2     220 Session Setup Request, NTLMSSP_NEGOTIATE
 11 0.002910    192.168.79.44    192.168.214.56   SMB2     309 Session Setup Response, Error: STATUS_MORE_PROCE
 12 0.003510    192.168.214.56   192.168.79.44    SMB2     607 Session Setup Request, NTLMSSP_AUTH, User: KL514
 13 0.004337    192.168.79.44    192.168.214.56   SMB2     159 Session Setup Response
 14 0.004645    192.168.214.56   192.168.79.44    SMB2     170 Tree Connect Request Tree: \\192.168.79.44\IPC$
 15 0.005021    192.168.79.44    192.168.214.56   SMB2     138 Tree Connect Response
 17 0.005386    192.168.79.44    192.168.214.56   SMB2     194 Ioctl Response FSCTL_VALIDATE_NEGOTIATE_INFO
 18 0.005486    192.168.214.56   192.168.79.44    SMB2     178 Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
 19 0.005617    192.168.214.56   192.168.79.44    SMB2     190 Create Request File: lsarpc
 20 0.005843    192.168.79.44    192.168.214.56   SMB2     778 Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INF
 21 0.005980    192.168.79.44    192.168.214.56   SMB2     210 Create Response File: lsarpc
 22 0.006024    192.168.214.56   192.168.79.44    TCP       54 50282 → 445 [ACK] Seq=1591 Ack=1813 Win=525568 L
 23 0.006221    192.168.214.56   192.168.79.44    DCERPC   286 Bind: call_id: 2, Fragment: Single, 2 context it
 24 0.006554    192.168.79.44    192.168.214.56   SMB2     138 Write Response
 25 0.006638    192.168.214.56   192.168.79.44    SMB2     171 Read Request Len:1024 Off:0 File: lsarpc
 26 0.006937    192.168.79.44    192.168.214.56   DCERPC   230 Bind_ack: call_id: 2, Fragment: Single, max_xmit
 27 0.007055    192.168.214.56   192.168.79.44    LSARPC   282 lsa_OpenPolicy2 request
 28 0.007470    192.168.79.44    192.168.214.56   LSARPC   218 lsa_OpenPolicy2 response
 30 0.008079    192.168.79.44    192.168.214.56   LSARPC   342 lsa_LookupNames3 response
 32 0.008524    192.168.79.44    192.168.214.56   LSARPC   218 lsa_Close response
 33 0.008617    192.168.214.56   192.168.79.44    SMB2     146 Close Request File: lsarpc
```



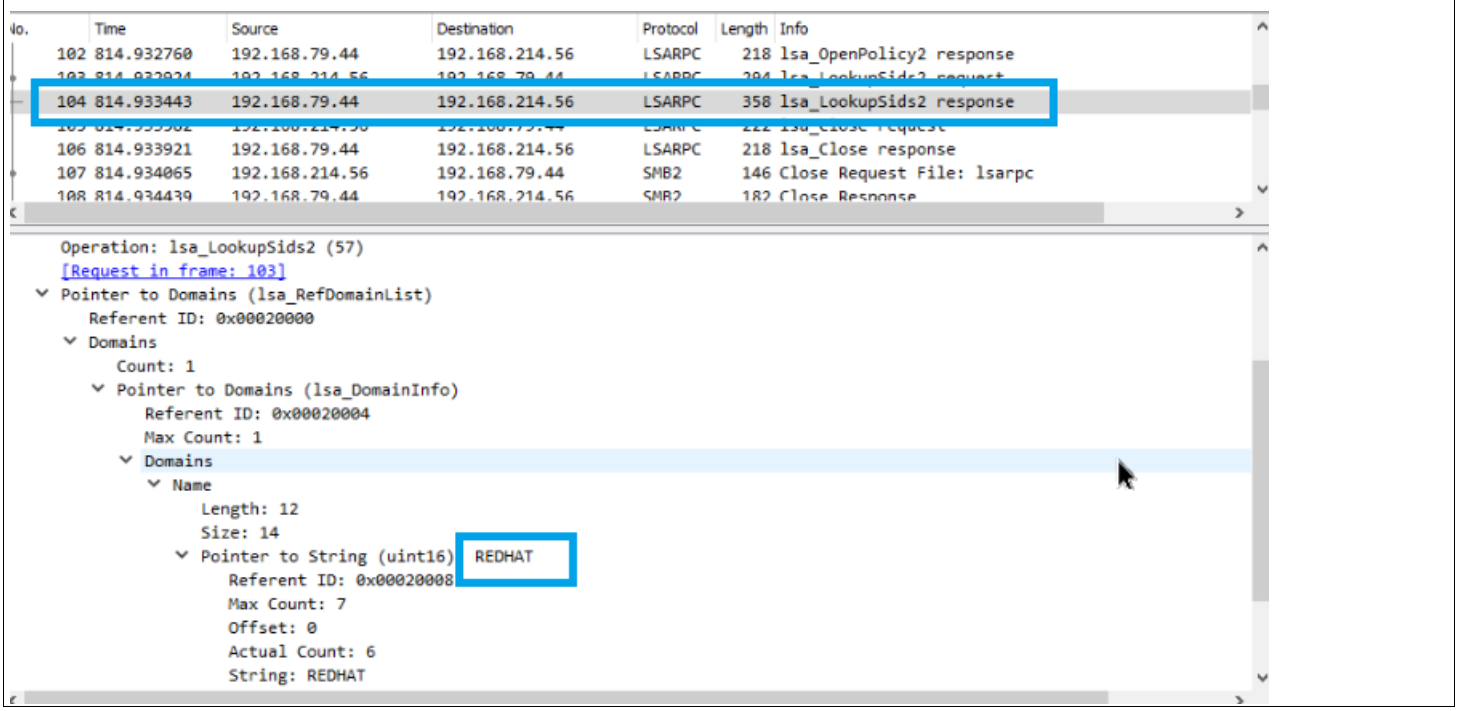
7.3a. (poniżej) Obraz okna prezentującego raporty uzyskane podczas realizacji kroków 11 oraz 12.
W zamieszczonym oknie powinny być widoczne i zaznaczone linie zawierające polecenia uruchomienia programu ***whoami*** oraz programu ***sid2user***

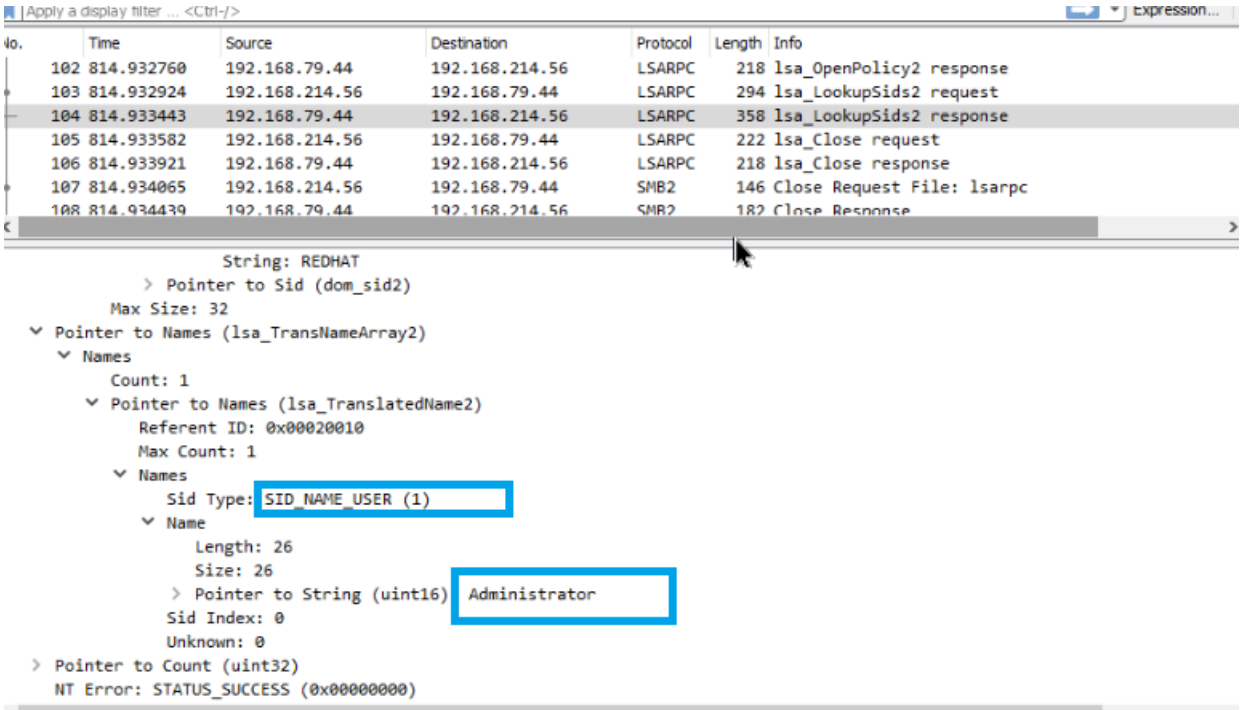


```
C:\Program Files (x86)\soft\win_sid>whoami
kl514\intruz_514

C:\Program Files (x86)\soft\win_sid>sid2user \\192.168.79.44 5 21 2923026099 4281651779 1442611520 1001

Name is TelnetClients
Domain is REDHAT
Type of SID is SidTypeAlias

C:\Program Files (x86)\soft\win_sid>sid2user \\192.168.79.44 5 21 2923026099 4281651779 1442611520 1002

Name is Kopciuch
Domain is REDHAT
Type of SID is SidTypeUser

C:\Program Files (x86)\soft\win_sid>sid2user \\192.168.79.44 5 21 2923026099 4281651779 1442611520 1003

Name is Waldek
Domain is REDHAT
Type of SID is SidTypeUser

C:\Program Files (x86)\soft\win_sid>sid2user \\192.168.79.44 5 21 2923026099 4281651779 1442611520 1004

LookupSidName failed - no such account

C:\Program Files (x86)\soft\win_sid>
```

7.3b. (poniżej) Obraz okna sniffera uzyskany podczas realizacji jednego z testów w kroku 12.
Kolorem niebieskim zaznaczono w panelu listy pakietów (*Packet List*), pakiet zawierający zwracane dane enumeracyjne. W panelu szczegółów (*Packet Details),* kolorem niebieskim zaznaczono zwrócone dane enumeracyjne.

Wkleić obraz okna





7.4. Opis zaobserwowanych efektów oraz wnioski dotyczące zadania:

Jm.in. opisy określone w instrukcji kolorem zielonym, w tym dokładny opis uzyskanych informacji oraz charakterystyka ruchu sieciowego obserwowanego podczas badania.

Z otrzymanych raportów można uzyskać infomacje takie jak:

-dla programu user2id: dla podanej nazwy użytkownika podaje SID systemu w którym użytkownik jest zapisany

-dla programu sid2user: dla podanego numeru SID + RID użytkownika systemu program podaje nazwę użytkownika

Z wyników realizacji ćwiczenia można wyciągnąć wnioski ,że użytkownik o numerze RID: 502 nie istnieje.

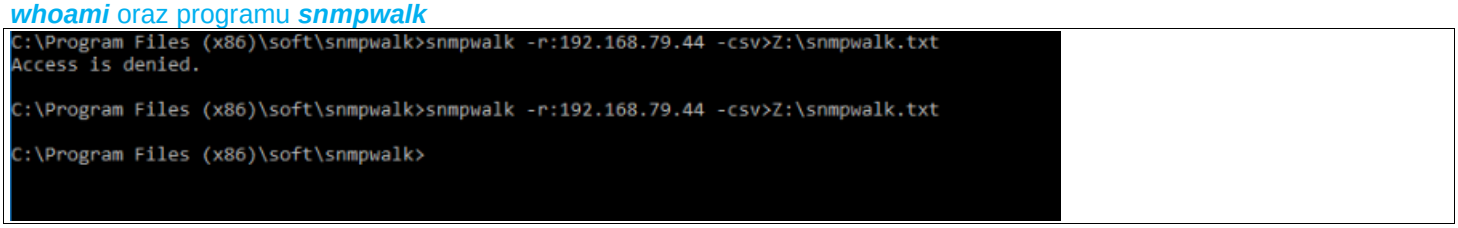
Użytkownik Kopciuch posiada RID: 1002, Waldek 1003

Użycie programu wymaga znajomości konta użytkownika znajdującego się na serwerze(INTRUZ ma odpowiednik w systemie enumerowanym).

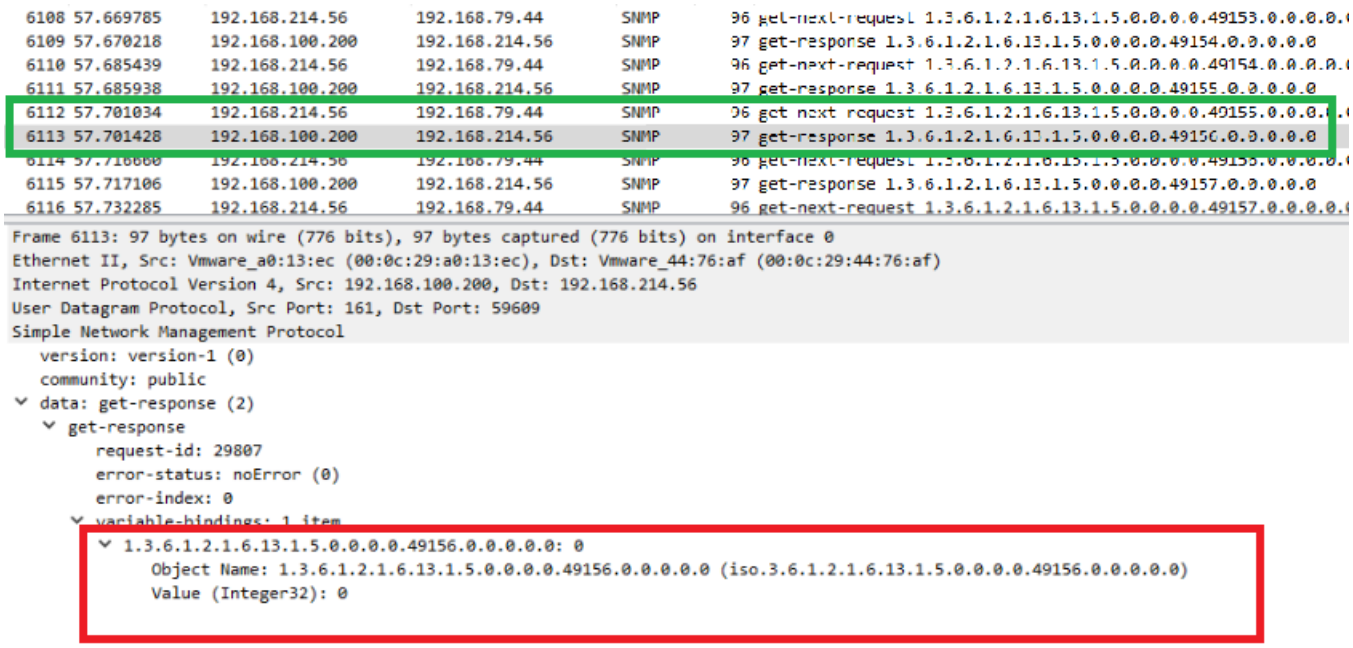
Zadanie 8 – Enumeracja za pomocą programu ***snmpwalk***

8.1 (poniżej) Obraz okna prezentującego raporty uzyskane podczas realizacji kroków 4 oraz 5.

W zamieszczonym oknie powinny być widoczne i zaznaczone linie zawierające polecenia uruchomienia programu ***whoami*** oraz programu ***snmpwalk***



8.2 (poniżej) Obraz okna sniffera uzyskany podczas badania przeprowadzonego w kroku 5. Kolorem zielonym zaznaczono w panelu listy pakietów (*Packet List*), dowolną jedną parę pakietów zawierających żądanie i zwrócone dane dotyczące jednego z kont użytkowników. W panelu szczegółów (*Packet Details i Packet Bytes),* kolorem czerwonym zaznaczono zwrócone dane dotyczące konta użytkownika zawarte w tym pakiecie.



8.3 (poniżej) Cztery fragmenty uzyskanego raportu prezentujące fragmenty sekcji dotyczących: kont użytkowników, listy procesów, listy usług, listy zainstalowanego oprogramowaniua. Dla każdegi fragmentu należy zamieścić opis informujący o rodzaju uzyskanych danych.

Konta użytkowników:

```
.1.3.6.1.4.1.77.1.2.25.1.1.5.71.117.101.115.116,OctetString,Guest
.1.3.6.1.4.1.77.1.2.25.1.1.6.87.97.108.100.101.107,OctetString,Waldek
.1.3.6.1.4.1.77.1.2.25.1.1.7.115.116.117.100.101.110.116,OctetString,student
.1.3.6.1.4.1.77.1.2.25.1.1.8.73.77.69.95.85.83.69.82,OctetString,IME_USER
.1.3.6.1.4.1.77.1.2.25.1.1.8.75.111.112.99.105.117.99.104,OctetString,Kopciuch
.1.3.6.1.4.1.77.1.2.25.1.1.9.73.77.69.95.65.68.77.73.78,OctetString,IME_ADMIN
.1.3.6.1.4.1.77.1.2.25.1.1.10.73.78.84.82.85.90.95.50.48.49,OctetString,INTRUZ_201
.1.3.6.1.4.1.77.1.2.25.1.1.10.73.78.84.82.85.90.95.50.48.50,OctetString,INTRUZ_202
.1.3.6.1.4.1.77.1.2.25.1.1.10.73.78.84.82.85.90.95.50.48.51,OctetString,INTRUZ_203
.1.3.6.1.4.1.77.1.2.25.1.1.10.73.78.84.82.85.90.95.50.48.52,OctetString,INTRUZ_204
.1.3.6.1.4.1.77.1.2.25.1.1.10.73.78.84.82.85.90.95.50.48.53,OctetString,INTRUZ_205
.1.3.6.1.4.1.77.1.2.25.1.1.10.73.78.84.82.85.90.95.50.48.54,OctetString,INTRUZ_206
.1.3.6.1.4.1.77.1.2.25.1.1.10.73.78.84.82.85.90.95.50.48.55,OctetString,INTRUZ_207
.1.3.6.1.4.1.77.1.2.25.1.1.10.73.78.84.82.85.90.95.50.48.56,OctetString,INTRUZ_208
.1.3.6.1.4.1.77.1.2.25.1.1.10.73.78.84.82.85.90.95.50.48.57,OctetString,INTRUZ_209
.1.3.6.1.4.1.77.1.2.25.1.1.10.73.78.84.82.85.90.95.50.49.48,OctetString,INTRUZ_210
.1.3.6.1.4.1.77.1.2.25.1.1.10.73.78.84.82.85.90.95.50.49.49,OctetString,INTRUZ_211
.1.3.6.1.4.1.77.1.2.25.1.1.10.73.78.84.82.85.90.95.50.49.50,OctetString,INTRUZ_212
.1.3.6.1.4.1.77.1.2.25.1.1.10.73.78.84.82.85.90.95.50.49.51,OctetString,INTRUZ_213
.1.3.6.1.4.1.77.1.2.25.1.1.10.73.78.84.82.85.90.95.50.49.53,OctetString,INTRUZ_215
```

Lista usług:

```
.1.3.6.1.4.1.77.1.2.3.1.1.4.87.73.78.83,OctetString,WINS
.1.3.6.1.4.1.77.1.2.3.1.1.5.80.111.119.101.114,OctetString,Power
.1.3.6.1.4.1.77.1.2.3.1.1.6.83.101.114.118.101.114,OctetString,Server
.1.3.6.1.4.1.77.1.2.3.1.1.6.84.101.108.110.101.116,OctetString,Telnet
.1.3.6.1.4.1.77.1.2.3.1.1.6.84.104.101.109.101.115,OctetString,Themes
.1.3.6.1.4.1.77.1.2.3.1.1.9.73.80.32.72.101.108.112.101.114,OctetString,IP Helper
.1.3.6.1.4.1.77.1.2.3.1.1.9.83.78.77.80.32.84.114.97.112,OctetString,SNMP Trap
.1.3.6.1.4.1.77.1.2.3.1.1.10.68.78.83.32.67.108.105.101.110.116,OctetString,DNS Client
.1.3.6.1.4.1.77.1.2.3.1.1.11.68.72.67.80.32.67.108.105.101.110.116,OctetString,DHCP Client
.1.3.6.1.4.1.77.1.2.3.1.1.11.87.111.114.107.115.116.97.116.105.111.110,OctetString,Worksta
.1.3.6.1.4.1.77.1.2.3.1.1.12.83.78.77.80.32.83.101.114.118.105.99.101,OctetString,SNMP Ser
.1.3.6.1.4.1.77.1.2.3.1.1.12.86.77.119.97.114.101.32.84.111.111.108.115,OctetString,VMware
.1.3.6.1.4.1.77.1.2.3.1.1.12.87.105.110.100.111.119.115.32.84.105.109.101,OctetString,Wind
.1.3.6.1.4.1.77.1.2.3.1.1.13.80.108.117.103.32.97.110.100.32.80.108.97.121,OctetString,Plu
.1.3.6.1.4.1.77.1.2.3.1.1.13.80.114.105.110.116.32.83.112.111.111.108.101.114,OctetString,
.1.3.6.1.4.1.77.1.2.3.1.1.14.84.97.115.107.32.83.99.104.101.100.117.108.101.114,OctetStrin
.1.3.6.1.4.1.77.1.2.3.1.1.15.83.101.99.111.110.100.97.114.121.32.76.111.103.111.110,OctetS
```

Lista Procesów:

```
.1.3.6.1.2.1.25.4.2.1.2.1,OctetString,System Idle Process
.1.3.6.1.2.1.25.4.2.1.2.4,OctetString,System
.1.3.6.1.2.1.25.4.2.1.2.236,OctetString,smss.exe
.1.3.6.1.2.1.25.4.2.1.2.324,OctetString,svchost.exe
.1.3.6.1.2.1.25.4.2.1.2.352,OctetString,csrss.exe
.1.3.6.1.2.1.25.4.2.1.2.420,OctetString,csrss.exe
.1.3.6.1.2.1.25.4.2.1.2.428,OctetString,wininit.exe
.1.3.6.1.2.1.25.4.2.1.2.456,OctetString,winlogon.exe
.1.3.6.1.2.1.25.4.2.1.2.524,OctetString,services.exe
.1.3.6.1.2.1.25.4.2.1.2.532,OctetString,lsass.exe
.1.3.6.1.2.1.25.4.2.1.2.640,OctetString,svchost.exe
.1.3.6.1.2.1.25.4.2.1.2.680,OctetString,svchost.exe
.1.3.6.1.2.1.25.4.2.1.2.740,OctetString,svchost.exe
.1.3.6.1.2.1.25.4.2.1.2.764,OctetString,spoolsv.exe
.1.3.6.1.2.1.25.4.2.1.2.784,OctetString,dwm.exe
.1.3.6.1.2.1.25.4.2.1.2.808,OctetString,svchost.exe
.1.3.6.1.2.1.25.4.2.1.2.864,OctetString,svchost.exe
.1.3.6.1.2.1.25.4.2.1.2.940,OctetString,svchost.exe
.1.3.6.1.2.1.25.4.2.1.2.956,OctetString,METray.exe
.1.3.6.1.2.1.25.4.2.1.2.1012,OctetString,cmd.exe
.1.3.6.1.2.1.25.4.2.1.2.1068,OctetString,armsvc.exe
.1.3.6.1.2.1.25.4.2.1.2.1092,OctetString,svchost.exe
.1.3.6.1.2.1.25.4.2.1.2.1116,OctetString,svchost.exe
.1.3.6.1.2.1.25.4.2.1.2.1136,OctetString,inetinfo.exe
```

Lista oprogramowania:

```
.1.3.6.1.2.1.25.6.3.1.1.16,Integer,16
.1.3.6.1.2.1.25.6.3.1.1.17,Integer,17
.1.3.6.1.2.1.25.6.3.1.2.1,OctetString,Microsoft Visual C++ 2010  x64 Redistributable - 10.0.40219
.1.3.6.1.2.1.25.6.3.1.2.2,OctetString,Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.4148
.1.3.6.1.2.1.25.6.3.1.2.3,OctetString,Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161
.1.3.6.1.2.1.25.6.3.1.2.4,OctetString,ArGoSoft Mail Server .NET
.1.3.6.1.2.1.25.6.3.1.2.5,OctetString,VMware Tools
.1.3.6.1.2.1.25.6.3.1.2.6,OctetString,Adobe Flash Player 10 ActiveX
.1.3.6.1.2.1.25.6.3.1.2.7,OctetString,Google Chrome
.1.3.6.1.2.1.25.6.3.1.2.8,OctetString,MailEnable Messaging Services for Microsoft Windows
.1.3.6.1.2.1.25.6.3.1.2.9,OctetString,OpenTFTPServer
.1.3.6.1.2.1.25.6.3.1.2.10,OctetString,WinPcap 4.1.3
.1.3.6.1.2.1.25.6.3.1.2.11,OctetString,Wireshark 1.10.0 (64-bit)
.1.3.6.1.2.1.25.6.3.1.2.12,OctetString,Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148
.1.3.6.1.2.1.25.6.3.1.2.13,OctetString,Google Update Helper
.1.3.6.1.2.1.25.6.3.1.2.14,OctetString,Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161
.1.3.6.1.2.1.25.6.3.1.2.15,OctetString,OpenOffice.org 3.4.1
.1.3.6.1.2.1.25.6.3.1.2.16,OctetString,Adobe Reader XI (11.0.01)
.1.3.6.1.2.1.25.6.3.1.2.17,OctetString,Microsoft SQL Server Compact 3.5 ENU
.1.3.6.1.2.1.25.6.3.1.3.1,OID,0.0
.1.3.6.1.2.1.25.6.3.1.3.2,OID,0.0
```

8.4 Opis zaobserwowanych efektów oraz wnioski dotyczące zadania:

m.in. opisy określone w instrukcji kolorem zielonym, w tym dokładny opis uzyskanych informacji oraz charakterystyka ruchu sieciowego obserwowanego podczas badania.

System Windows może udostępniać informacje jeżeli zostanie na nim uruchomiony agent SNMP. Dostęp do badanego komputera nie wymaga uwierzytelnienia, jestem w stanie uruchomić program snmpwalk z konta tester. Wygenerowany przez program snmpwalk raport zawiera mnóstwo informacji na temat serwera stanowiące poważne zagrożenie dla bezpieczeństwa. W raporcie możemy odnaleźć informacje takie jak:

- uruchomione usługi,
- nazwy zasobów sieciowych,
- nazwy użytkowników,
- nazwy domen,
- nazwy komputerów,
- informacje o zainstalowanym oprogramowaniu

Do uzyskania informacji został wykorzystany protokół SNMP.

Własne uwagi, wnioski i propozycje dotyczące przebiegu ćwiczenia, mające na celu polepszenie procesu kształcenia:

Wydłużony czas o godzinę , sprawozdanie powinienem wysłać do 14.30