

## 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 zrealizowaniu zadania 1](#)

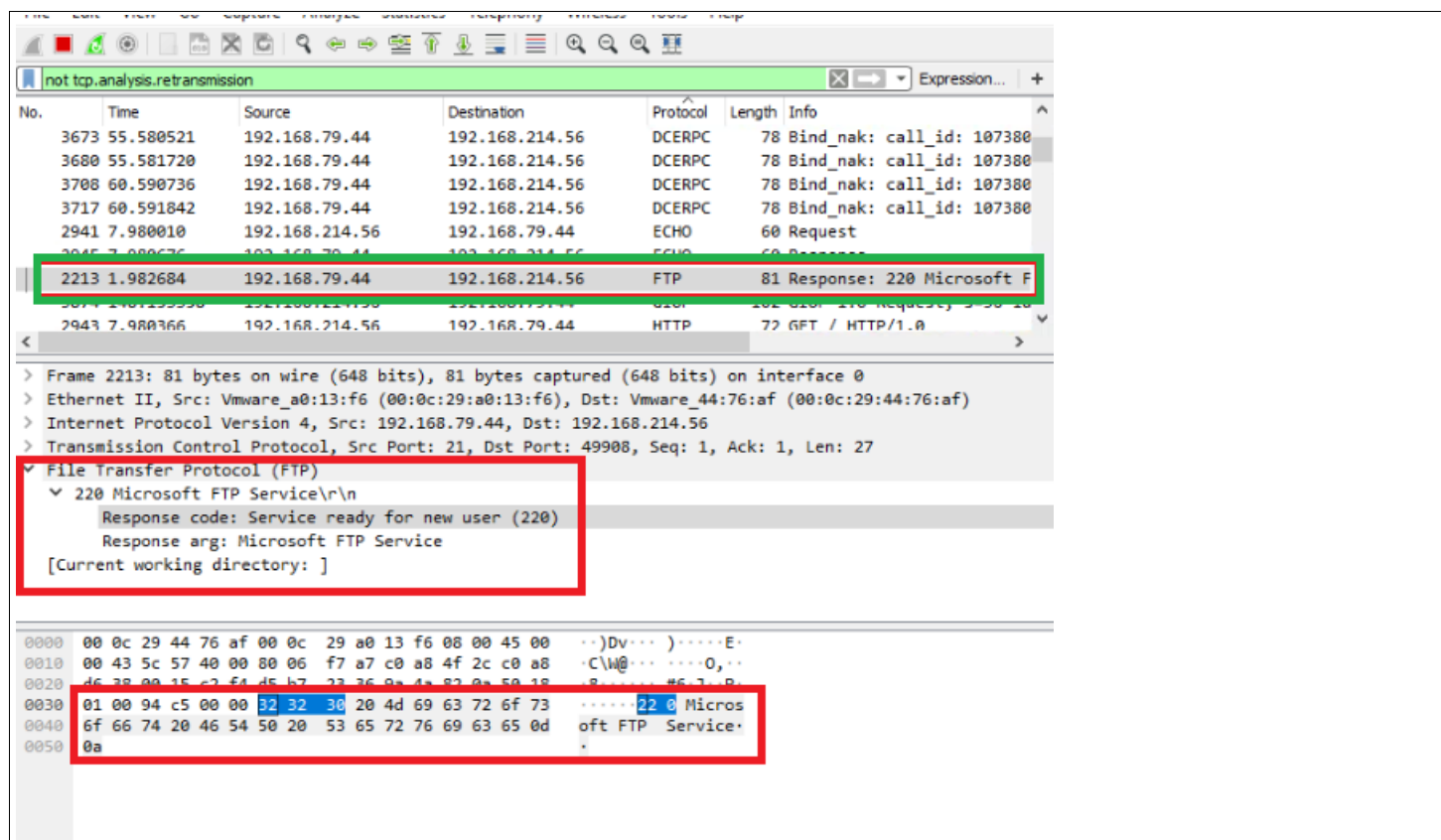
### Zadanie 2 – Pozyskiwanie banerów aplikacji za pomocą programu *nmap*

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

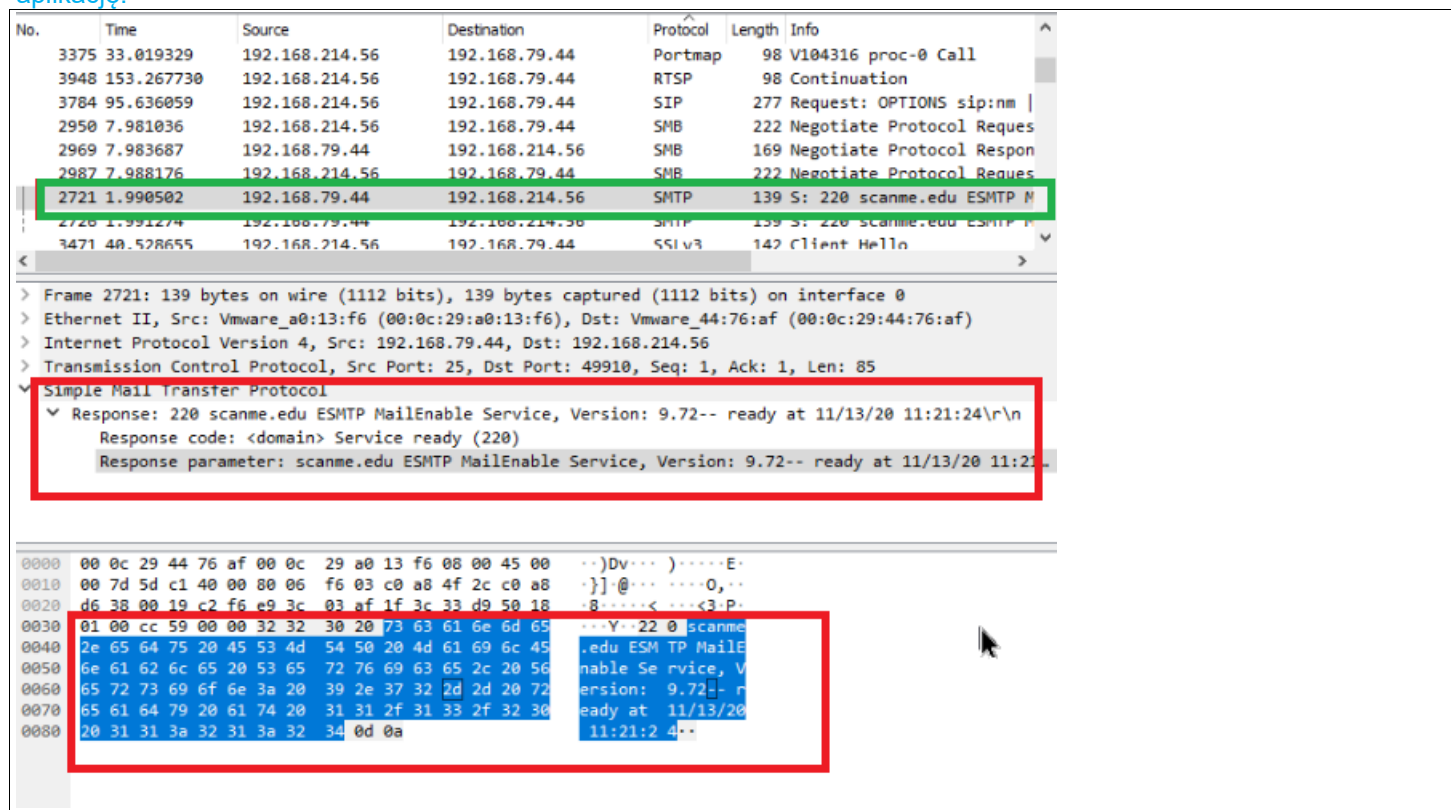
```
C:\Users\Administrator>nmap -SV 192.168.79.44
Starting Nmap 7.70 ( https://nmap.org ) at 2020-11-13 12:37 Central European Standard Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or spe
cify valid servers with --dns-servers
Nmap scan report 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 smtpd 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 smtpd 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%T=7%O=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.

No.	Time	Source	Destination	Protocol	Length	Info
2943	7.980366	192.168.214.56	192.168.79.44	HTTP	72	GET / HTTP/1.0
2953	7.981222	192.168.214.56	192.168.79.44	HTTP	107	GET /nice%20ports%2C/Tri%20
2974	7.986349	192.168.79.44	192.168.214.56	HTTP	259	HTTP/1.1 200 OK (text/html)
3046	12.982152	192.168.214.56	192.168.79.44	HTTP	72	GET / HTTP/1.0
3059	12.982996	192.168.214.56	192.168.79.44	HTTP	72	GET / HTTP/1.0
3060	12.983159	192.168.214.56	192.168.79.44	HTTP	72	GET / HTTP/1.0
3061	12.983308	192.168.214.56	192.168.79.44	HTTP	72	GET / HTTP/1.0
3062	12.983439	192.168.214.56	192.168.79.44	HTTP	72	GET / HTTP/1.0
3115	17.999060	192.168.214.56	192.168.79.44	HTTP	76	OPTIONS / HTTP/1.0

Transmission Control Protocol, Src Port: 80, Dst Port: 49912, Seq: 1461, Ack: 19, Len: 205						
[2 Reassembled TCP Segments (1665 bytes): #2973(1460)...#2974(205)]						
Hypertext Transfer Protocol						
HTTP/1.1 200 OK\r\n						
Content-Type: text/html\r\n						
Last-Modified: Sat, 11 Feb 2017 20:10:57 GMT\r\n						
Accept-Ranges: bytes\r\n						
ETag: "d8dec8f4a284d21:0"\r\n						
Server: Microsoft-IIS/8.0\r\n						
Date: Fri, 13 Nov 2020 10:21:30 GMT\r\n						

0080	34 64 32 31 3a 30 22 0d 0a 53 65 72 76 65 72 3e	4d21:0" Server:
0090	20 4d 69 63 72 6f 73 6f 66 74 2d 49 49 53 2f 38	Microsoft-IIS/8
00a0	2e 30 0d 0a 58 2d 50 6f 77 65 72 65 64 2d 42 79	.0.X-Powered-By
00b0	3a 20 41 33 30 2e 4e 43 34 0d 0a 44 01 74 03 3a	ASP.NET Date:
00c0	20 46 72 69 2c 20 31 33 20 4e 6f 76 20 32 30 32	Fri, 13 Nov 202
00d0	30 20 31 30 3a 32 31 3a 33 30 20 47 4d 54 0d 0a	0 10:21: 30 GMT
00e0	43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 63 6c 6f 73	Connection: clos
00f0	65 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74	Content-Lengt
0100	68 3a 20 31 33 39 38 0d 0a 0d 0a 3c 21 44 4f 43	h: 1398: <<<DOC
0110	54 59 50 45 20 48 54 4d 4c 3e 0d 0a 3c 68 74 6d	TYPE HTML>>>htm
0120	6c 3e 0d 0a 09 3c 68 65 61 64 3e 0d 0a 09 09 3c	l>>>thead>>>

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

Administrator: Command Prompt	
: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 155.39 seconds	
C:\Program Files (x86)\Nmap>nmap -sT -p 21378 -PN 192.168.79.44	
Starting Nmap 7.70 (https://nmap.org) at 2020-11-13 10:54 Central European Standard Time	
nass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --	
cify valid servers with --dns-servers	
Nmap scan report for 192.168.79.44	
Host is up (0.00s latency).	
PORT	STATE SERVICE
21378/tcp	open unknown
Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds	
C:\Program Files (x86)\Nmap>	

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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Vmware_a0:13:f6	Broadcast	ARP	60	Who has 192.168.214.56? Tell 192.168.79
2	0.000030	Vmware_44:76:af	Vmware_a0:13:f6	ARP	42	192.168.214.56 is at 00:0c:29:44:76:af
3	0.000702	192.168.79.44	192.168.214.56	NBSS	60	NBSS Continuation Message
4	0.000766	192.168.214.56	192.168.79.44	TCP	66	49748 → 445 [ACK] Seq=1 Ack=2 Win=12178
5	4.524847	Vmware_44:76:af	Vmware_a0:13:f6	ARP	42	Who has 192.168.79.44? Tell 192.168.214
6	18.659197	192.168.214.56	192.168.79.44	TCP	66	50057 → 21378 [SYN] Seq=0 Win=8192 Len=
7	18.660016	192.168.79.44	192.168.214.56	TCP	66	21378 → 50057 [SYN, ACK] Seq=0 Ack=1 W
8	18.660054	192.168.214.56	192.168.79.44	TCP	54	50057 → 21378 [ACK] Seq=1 Ack=1 Win=52
9	18.665427	192.168.214.56	192.168.79.44	TCP	54	50057 → 21378 [RST, ACK] Seq=1 Ack=1 W
10	120.016440	Vmware_44:76:af	Broadcast	ARP	60	Who has 192.168.214.56? Tell 192.168.79
11	120.016841	192.168.79.44	192.168.214.56	TCP	60	[TCP Keep-Alive] 445 → 49748 [ACK] Seq=
12	120.016889	192.168.214.56	192.168.79.44	TCP	66	[TCP Keep-Alive ACK] 49748 → 445 [ACK]
13	124.527715	Vmware_44:76:af	Vmware_a0:13:f6	ARP	42	Who has 192.168.79.44? Tell 192.168.214
14	124.528129	Vmware_a0:13:f6	Vmware_44:76:af	ARP	60	192.168.79.44 is at 00:0c:29:a0:13:f6

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



Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds

C:\Program Files (x86)\Nmap>nmap -A 192.168.79.44

Starting Nmap 7.70 ( <https://nmap.org> ) at 2020-11-13 10:37 Central European Standard Time  
 mass\_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --sys-  
 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?	
--------	------	----------	--

| fingerprint-strings:

| NULL, RTSPRequest:

| 11:37:48 2020-11-13

17/tcp	open	qotd	Windows qotd (English)
--------	------	------	------------------------

19/tcp	open	chargen	
--------	------	---------	--

21/tcp	open	ftp	Microsoft ftpd
--------	------	-----	----------------

| ftp-syst:

| SYST: Windows\_NT

23/tcp	open	telnet	Microsoft Windows XP telnetd
--------	------	--------	------------------------------

| telnet-ntlm-info:

| Target\_Name: REDHAT

| NetBIOS\_Domain\_Name: REDHAT

| NetBIOS\_Computer\_Name: REDHAT

| DNS\_Domain\_Name: RedHat

| DNS\_Computer\_Name: RedHat

| Product\_Version: 6.2.9200

25/tcp	open	smtp	MailEnable smtpd 9.72--
--------	------	------	-------------------------

| smtp-commands: scanme.edu [192.168.214.56], this server offers 4 extensions, AUTH LOGIN, SIZE

| AUTH=LOGIN,

| 211 Help:->Supported Commands: HELO,EHLO,QUIT,HELP,RCPT,MAIL,DATA,RSET,NOOP

42/tcp	open	tcpwrapped	
--------	------	------------	--

80/tcp	open	http	Microsoft IIS httpd 8.0
--------	------	------	-------------------------

| http-methods:

| Potentially risky methods: TRACE

|\_http-server-header: Microsoft-IIS/8.0

|\_http-title: Microsoft Internet Information Services 8

110/tcp	open	pop3	MailEnable POP3 Server
---------	------	------	------------------------

|\_pop3-capabilities: USER TOP UIDL

135/tcp	open	msrpc	Microsoft Windows RPC
---------	------	-------	-----------------------

139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
---------	------	-------------	-------------------------------

|\_DNS\_Computer\_Name: RedHat

|\_Product\_Version: 6.2.9200

25/tcp	open	smtp	MailEnable smtpd 9.72--
--------	------	------	-------------------------

| smtp-commands: scanme.edu [192.168.214.56], this server offers 4 extensions, AUTH LOGIN, SIZE

| AUTH=LOGIN,

| 211 Help:->Supported Commands: HELO,EHLO,QUIT,HELP,RCPT,MAIL,DATA,RSET,NOOP

42/tcp	open	tcpwrapped	
--------	------	------------	--

80/tcp	open	http	Microsoft IIS httpd 8.0
--------	------	------	-------------------------

| http-methods:

| Potentially risky methods: TRACE

|\_http-server-header: Microsoft-IIS/8.0

|\_http-title: Microsoft Internet Information Services 8

110/tcp	open	pop3	MailEnable POP3 Server
---------	------	------	------------------------

|\_pop3-capabilities: USER TOP UIDL

135/tcp	open	msrpc	Microsoft Windows RPC
---------	------	-------	-----------------------

139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
---------	------	-------------	-------------------------------

143/tcp	open	imap	MailEnable imapd
---------	------	------	------------------

|\_imap-capabilities: IDLE IMAP4rev1 CHILDREN AUTH=LOGIN completed CAPABILITY OK IMAP4 AUTH=CRAM-

445/tcp	open	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
---------	------	--------------	--

587/tcp	open	smtp	MailEnable smtpd 9.72--
---------	------	------	-------------------------

| smtp-commands: scanme.edu [192.168.214.56], this server offers 4 extensions, AUTH LOGIN, SIZE

| AUTH=LOGIN,

| 211 Help:->Supported Commands: HELO,EHLO,QUIT,HELP,RCPT,MAIL,DATA,RSET,NOOP

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 th

ngerprint at <https://nmap.org/cgi-bin/submit.cgi?new-service> :

SF-Port13-TCP:V=7.70%I=7%D=11/13%Time=5FAE53EC%P=i686-pc-windows-windows%r

SF:(NULL,14,"11:37:48\x202020-11-13\n")%r(RTSPRequest,14,"11:37:48\x202020

SF:-11-13\n");

MAC Address: 00:0C:29:A0:13:F6 (VMware)

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:mic

.8.1

OS details: Microsoft Windows Server 2012 R2 Update 1, Microsoft Windows 7, Windows Server 2012,

1 Update 1

Network Distance: 1 hop

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 specify 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 sniffiera 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 sniffiera 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.

### 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**

```
C:\Users\TESTER_514>whoami
kl514\tester_514

C:\Users\TESTER_514>nbtscan -f -v 192.168.79.44
'nbtscan' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\TESTER_514>cd C:\Program Files (x86)\soft\nbtscan

C:\Program Files (x86)\soft\nbtscan>nbtscan -f -v 192.168.79.44
Using Winsock 2.2
Bound to 0.0.0.0.0
sending to 192.168.79.44
Got 157 bytes from 192.168.79.44
192.168.79.44    WORKGROUP\REDHAT    SHARING
  REDHAT        <00> UNIQUE Workstation Service
  WORKGROUP     <00> GROUP  Domain Name
  REDHAT        <20> UNIQUE File Server Service
  00:0c:29:a0:13:f6  ETHER  REDHAT

C:\Program Files (x86)\soft\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.

Time	Source	Destination	Protocol	Length	Info
1 0.000000	192.168.214.56	192.168.79.44	NBNS	92	Name query NBSTAT *(<00><00><00><00><00><00>
2 0.000492	192.168.79.44	192.168.214.56	NBNS	199	Name query response NBSTAT
3 0.000493	Vmware_a0:13:f6	Broadcast	ARP	60	who has 192.168.214.56? Tell 192.168.79.44
4 0.000523	Vmware_44:76:af	Vmware_a0:13:f6	ARP	42	192.168.214.56 is at 00:0c:29:44:76:af
5 0.068038	192.168.214.56	192.168.79.44	NBNS	92	Name query NBSTAT *(<00><00><00><00><00><00>
6 0.068611	192.168.79.44	192.168.214.56	NBNS	199	Name query response NBSTAT
7 4.821098	Vmware_44:76:af	Vmware_a0:13:f6	ARP	42	who has 192.168.79.44? Tell 192.168.214.56
8 4.821581	Vmware_a0:13:f6	Vmware_44:76:af	ARP	60	192.168.79.44 is at 00:0c:29:a0:13:f6

Flags: 0x8400, Response, Opcode: Name query, Authoritative, Reply code: No error

Questions: 0

Answer RRs: 1

Authority RRs: 0

Additional RRs: 0

## Answers

[illegible][illegible]

Type: NBSTAT (33)

Class: IN (1)

Time to live: 0 seconds

Data length: 101

Number of names: 3

Name: REDHAT&lt;00&gt; (Workstation/Redirector)

Downloaded from <http://ajphaphysocpharm.sagepub.com/> at 11:56 11 November 2014

Name: WORKGROUP<00> (Workstation/Redirector)

```
> Name + Age: MycDADA Name type: Unknown, Name is active
```

Name: REDHAT<20> (Server service)

```
> name: Plug-in error, only unknown, name is active
```

Unit ID: Vmware\_a0:13:f6 (00:0c:29:a0:13:f6)

Jumpers: 0x00

#### 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.





```

C:\Users\INTRUZ_514>whoami
INTRUZ_514

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

C:\Program Files (x86)\soft>userinfo \\192.168.79.44 INTRUZ_514

UserInfo v1.5 - thor@hammerofgod.com

Querying Controller \\192.168.79.44

USER INFO
Username:      INTRUZ_514
Full Name:     INTRUZ_014
Comment:
User Comment:
User ID:       1020
Primary Grp:   513
Privs:         User Privs
OperatorPrivs: No explicit OP Privs

SYSTEM FLAGS (Flag dword is 66113)
User cannot change password.
User's pwd never expires.

MISC INFO
Password age:  Mon May 15 20:45:31 2017
LastLogon:     Fri Nov 13 11:18:18 2020
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

SYSTEM FLAGS (Flag dword is 66113)
User cannot change password.
User's pwd never expires.

MISC INFO
Password age:  Mon May 15 20:45:31 2017
LastLogon:     Fri Nov 13 11:18:18 2020
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!

C:\Program Files (x86)\soft>

```

**Oraz dla Guest:**



```

C:\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         11111111111111111111111111111111
Monday         11111111111111111111111111111111
Tuesday        11111111111111111111111111111111
Wednesday      11111111111111111111111111111111
Thursday       11111111111111111111111111111111
Friday         11111111111111111111111111111111
Saturday       11111111111111111111111111111111

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.

Time	Source	Destination	Protocol	Length	Info
62 96.937719	192.168.214.56	192.168.79.44	SMB2	232	Negotiate Protocol Request
63 96.938400	192.168.79.44	192.168.214.56	SMB2	228	Negotiate Protocol Response
64 96.939605	192.168.214.56	192.168.79.44	SMB2	220	Session Setup Request, NTLMSSP_NEGOTIATE
65 96.940283	192.168.79.44	192.168.214.56	SMB2	309	Session Setup Response, Error: STATUS_MORE_PROCE
66 96.940751	192.168.214.56	192.168.79.44	SMB2	607	Session Setup Request, NTLMSSP_AUTH, User: KLS14
67 96.942612	192.168.79.44	192.168.214.56	SMB2	159	Session Setup Response
68 96.943044	192.168.214.56	192.168.79.44	SMB2	170	Tree Connect Request Tree: \\192.168.79.44\IPC\$
69 96.943783	192.168.79.44	192.168.214.56	SMB2	138	Tree Connect Response
70 96.943833	192.168.214.56	192.168.79.44	SMB2	212	Ioctl Request FSCTL_VALIDATE_NEGOTIATE_INFO
71 96.944368	192.168.79.44	192.168.214.56	SMB2	194	Ioctl Response FSCTL_VALIDATE_NEGOTIATE_INFO
72 96.944537	192.168.214.56	192.168.79.44	SMB2	178	Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
73 96.944597	192.168.214.56	192.168.79.44	SMB2	186	Create Request File: samr
74 96.945087	192.168.79.44	192.168.214.56	TCP	60	445 → 50276 [ACK] Seq=933 Ack=1587 Win=64256 Len

Chain Offset: 0x00000000  
Message ID: Unknown (4)  
Process ID: 0x0000feff  
Tree Id: 0x00000001 \\192.168.79.44\IPC\$  
[Tree: \\192.168.79.44\IPC\$]  
[Share Type: Named pipe (0x02)]  
[Connected in Frame: 69]  
Signature: 00000000000000000000000000000000  
[Response to: 68]  
[Time from request: 0.000739000 seconds]  
Tree Connect Response (0x03)

## 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
16	0.005054	192.168.79.44	192.168.214.56	SMB2	222 Ioctl Request FSCTL_VALIDATE_NEGOTIATE_INFO
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
29	0.007611	192.168.214.56	192.168.79.44	LSARPC	286 lsa_LookupNames3 request
30	0.008079	192.168.79.44	192.168.214.56	LSARPC	342 lsa_LookupNames3 response
31	0.008100	192.168.214.56	192.168.79.44	LSARPC	222 lsa_Close request
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



27 0.000000	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
29 0.007631	192.168.214.56	192.168.79.44	LSARPC	286 lsa_LookupNames3 request
30 0.008079	192.168.79.44	192.168.214.56	LSARPC	342 lsa_LookupNames3 response
31 0.008166	192.168.214.56	192.168.79.44	LSARPC	222 lsa_Close request
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	SMR2	146 Close Request File: lsarpc

```

Count: 1
  Pointer to Sids (lsa_TranslatedSid3)
    Referent ID: 0x00020010
    Max Count: 1
    Sids
      Sid Type: SID_NAME_DOMAIN (3)
      Pointer to Sid (dom_sid2)
        Referent ID: 0x00020014
        Count: 4
        Sid: 5-1-5-21-2923026099-4281651779-1442611520 (Domain SID)
          Revision: 1
          Num Auth: 4
          Authority: 5
          Subauthorities: 21-2923026099-4281651779-1442611520
          Sid Index: 0
          Unknown: 0
  Pointer to Count (uint32)
    Count: 1

```

29 0.007611	192.168.214.56	192.168.79.44	LSARPC	286 lsa_LookupNames3 request
30 0.008079	192.168.79.44	192.168.214.56	LSARPC	342 lsa_LookupNames3 response
31 0.008166	192.168.214.56	192.168.79.44	LSARPC	222 lsa_Close request
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	SMR2	146 Close Request File: lsarpc

```

[Request in frame: 29]
  Pointer to Domains (lsa_RefDomainList)
    Referent ID: 0x00020000
    Domains
      Count: 1
      Pointer to Domains (lsa_DomainInfo)
        Referent ID: 0x00020004
        Max Count: 1
        Domains
          Name
            Length: 12
            Size: 14
            > Pointer to String (uint16): REDHAT
            > Pointer to Sid (dom_sid2)
              Max Size: 32
        > Pointer to Sids (lsa_TransSidArray3)
        > Pointer to Count (uint32)
          Count: 1

```

**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 500

Name is Administrator
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 501

Name is Guest
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 502

LookupSidName failed - no such account

C:\Program Files (x86)\soft\win_sid>sid2user \\192.168.79.44 5 21 2923026099 4281651779 1442611520 1000

Name is WinRMRemoteWMIUsers__
Domain is REDHAT
Type of SID is SidTypeAlias

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

```

```
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

The image shows a Wireshark packet capture. The top pane, 'Packet List', displays a list of captured packets. Packet 104, at time 814.933443, is an LSA\_LOOKUPSID2 response from 192.168.79.44 to 192.168.214.56, with a length of 358 bytes. This packet is highlighted with a blue selection bar. The bottom pane, 'Packet Details', shows the structure of the selected packet. It is an 'Operation: lsa\_LookupSids2 (57)'. Under 'Pointer to Domains (lsa\_RefDomainList)', the 'Referent ID' is 0x00020000. Under 'Domains', the 'Count' is 1. Under 'Pointer to Domains (lsa\_DomainInfo)', the 'Referent ID' is 0x00020004 and 'Max Count' is 1. Under 'Domains', the 'Name' field is expanded, showing 'Length: 12', 'Size: 14', and 'Pointer to String (uint16)' pointing to 'REDHAT'. The 'String' field is also expanded, showing 'Actual Count: 6' and 'String: REDHAT'. The 'REDHAT' string is highlighted with a blue selection bar.

No.	Time	Source	Destination	Protocol	Length	Info
102	814.932760	192.168.79.44	192.168.214.56	LSARPC	218	lsa_OpenPolicy2 response
103	814.933034	192.168.214.56	192.168.79.44	LSARPC	204	lsa_LookupSids2 request
104	814.933443	192.168.79.44	192.168.214.56	LSARPC	358	lsa_LookupSids2 response
105	814.933502	192.168.214.56	192.168.79.44	LSARPC	222	lsa_Close request
106	814.933921	192.168.79.44	192.168.214.56	LSARPC	218	lsa_Close response
107	814.934065	192.168.214.56	192.168.79.44	SMB2	146	Close Request File: lsarpc
108	814.934439	192.168.79.44	192.168.214.56	SMB2	182	Close Response

Operation: lsa\_LookupSids2 (57)  
[Request in frame: 103]  
▼ Pointer to Domains (lsa\_RefDomainList)  
Referent ID: 0x00020000  
▼ Domains  
Count: 1  
▼ Pointer to Domains (lsa\_DomainInfo)  
Referent ID: 0x00020004  
Max Count: 1  
▼ Domains  
▼ Name  
Length: 12  
Size: 14  
▼ Pointer to String (uint16)  
Referent ID: 0x00020008  
Max Count: 7  
Offset: 0  
Actual Count: 6  
String: REDHAT

Apply a display filter ... <Ctrl-/> expression...

No.	Time	Source	Destination	Protocol	Length	Info
102	814.932760	192.168.79.44	192.168.214.56	LSARPC	218	lsa_OpenPolicy2 response
103	814.932924	192.168.214.56	192.168.79.44	LSARPC	294	lsa_LookupSids2 request
104	814.933443	192.168.79.44	192.168.214.56	LSARPC	358	lsa_LookupSids2 response
105	814.933582	192.168.214.56	192.168.79.44	LSARPC	222	lsa_Close request
106	814.933921	192.168.79.44	192.168.214.56	LSARPC	218	lsa_Close response
107	814.934065	192.168.214.56	192.168.79.44	SMB2	146	Close Request File: lsarpc
108	814.934439	192.168.79.44	192.168.214.56	SMB2	182	Close Response

String: REDHAT

- > Pointer to Sid (dom\_sid2)
  - Max Size: 32
- ▼ Pointer to Names (lsa\_TransNameArray2)
  - ▼ Names
    - Count: 1
    - ▼ Pointer to Names (lsa\_TranslatedName2)
      - Referent ID: 0x00020010
      - Max Count: 1
      - ▼ Names
        - Sid Type: **SID\_NAME\_USER (1)**
        - ▼ Name
          - Length: 26
          - Size: 26
          - > Pointer to String (uint16) **Administrator**
          - Sid Index: 0
          - Unknown: 0
- > Pointer to Count (uint32)

NT Error: STATUS\_SUCCESS (0x00000000)

#### 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 informacje 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 system 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**

```
C:\Program Files (x86)\soft\snmpwalk>snmpwalk -r:192.168.79.44 -csv>Z:\snmpwalk.txt
Access is denied.

C:\Program Files (x86)\soft\snmpwalk>snmpwalk -r:192.168.79.44 -csv>Z:\snmpwalk.txt

C:\Program Files (x86)\soft\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.





```
.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,OpenFTPServer
.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