

1 Laboratorium SNMP

1.1 Cel ćwiczenia

Celem ćwiczenia jest zapoznanie się z zarządzaniem urządzeniami sieciowymi za pomocą protokołu SNMP.

1.2 Informacje wstępne

SNMP to protokół zarządzania siecią działający w oparciu o TCP/IP. Podstawą systemu zarządzania siecią jest baza danych, czyli baza informacji zarządzania MIB. Obejmuje protokół wymiany danych, specyfikacje struktury baz danych oraz grupy obiektów danych. Łączy stacje zarządzania i agenty.

SNMPv1 jest najprostszą wersją protokołu SNMP. Umożliwia wykonywanie następujących funkcji: **GetRequest**, **GetNextRequest**, **GetResponse**, **SetRequest** i **Trap**. Do drugiej wersji protokołu wprowadzono ulepszenia funkcjonalne. **SNMPv2** został wzbogacony o nowe funkcje: **GetBulkRequest** i **InformRequest**. Procedury udostępniane przez oba protokoły ilustruje Tab. 1:

Tab. 1. Procedury udostępniane przez SNMPv1 oraz SNMPv2

Jednostka PDU	Opis
GetRequest	Pozwala na pobranie wartości obiektu skalarnego przez stację zarządzającą od stacji zarządzanej.
GetNextRequest	Bardzo podobna do PDU GetRequest, jednak jej wynikiem jest wartość instancji obiektu, która jest następną w porządku leksykograficznym po podanej w zapytaniu.
GetResponse	Są to odpowiedzi agenta na polecenia get lub set.
SetRequest	Daje możliwość zarządcy na ustawienie wartości obiektów w agencie.
Trap	Dzięki tej funkcji agent może powiadamiać stację zarządzania o ważnych zdarzeniach, mimo braku zapytania.
GetBulkRequest	Umożliwia odczyt wielu wartości w ramach jednego zapytania, co pozwala zminimalizować ilość transakcji.
InformRequest	Daje możliwość zarządcy na wysłanie zapytania do innej jednostki zarządzania. Powiadamia o stanie informacji zarządzania w innym zarządcy.

Komunikaty `GetRequest`, `GetNextRequest` i `GetBulkRequest` mają między sobą pewne różnice. Pierwszy z tych komunikatów pozwala na odczyt wartości każdego z przedstawionych obiektów. Drugi umożliwia odczyt następnej wartości każdego z obiektów. Natomiast `GetBulkRequest` pozwala uzyskać duży zakres danych w ramach jednego zapytania. Dzięki temu koszty są zdecydowanie mniejsze. Na powyższe zapytania agent odsyła komunikat `Response`.

Mimo, że obie wersje protokołu są do siebie bardzo podobne, to jednak ze względu na kilka istotnych różnic, nie mogą one ze sobą bezpośrednio współdziałać. Aby stało się to możliwe, należy użyć pełnomocników. Jest to najlepszy sposób na zapewnienie współpracy między protokołami. Można pomiędzy zarządcą SNMPv2 a agentem SNMPv1 ustawić pełnomocnika proxy. Będzie on dokonywał dwukierunkowej konwersji protokołów SNMPv1 oraz SNMPv2.

Innym sposobem na komunikację między SNMPv1 oraz SNMPv2 jest zastosowanie stacji zarządzania obsługującej obie powyższe wersje protokołu. Wtedy, gdy np. zarządca SNMPv2 będzie komunikować się z agentami SNMPv1, to zarządca wspierający obie wersje protokołu będzie pośredniczył w komunikacji podobnie jak robi to agent proxy.

SNMPv3 został poszerzony o funkcje bezpieczeństwa i funkcje administracyjne. W tej wersji protokołu pojawiły się następujące zabezpieczenia:

Szyfrowanie – możliwość zaszyfrowania komunikatów PDU SNMP za pomocą symetrycznego szyfru blokowego (ang. Data Encryption Standard – DES). Tajny klucz użytkownika, który szyfruje dane musi być również znany odbiorcy tych danych.

Uwierzytelnianie – do uwierzytelniania i ochrony przed modyfikacją danych stosowany jest kod uwierzytelniania wiadomości (ang. Message Authentication Code – MAC). Tutaj też tajny klucz musi być znany zarówno nadawcy jak i odbiorcy wiadomości.

Ochrona przed odtworzeniem – w SNMPv3 do każdego komunikatu nadawca dołącza wartość bazującą na liczniku, który istnieje u odbiorcy. Dzięki temu można upewnić się, że odebrany komunikat nie jest odtworzoną wersją komunikatu wysłanego wcześniej. Komunikat jest akceptowany, jeśli wartość licznika w otrzymanej wiadomości jest w miarę podobna do rzeczywistej wartości licznika.

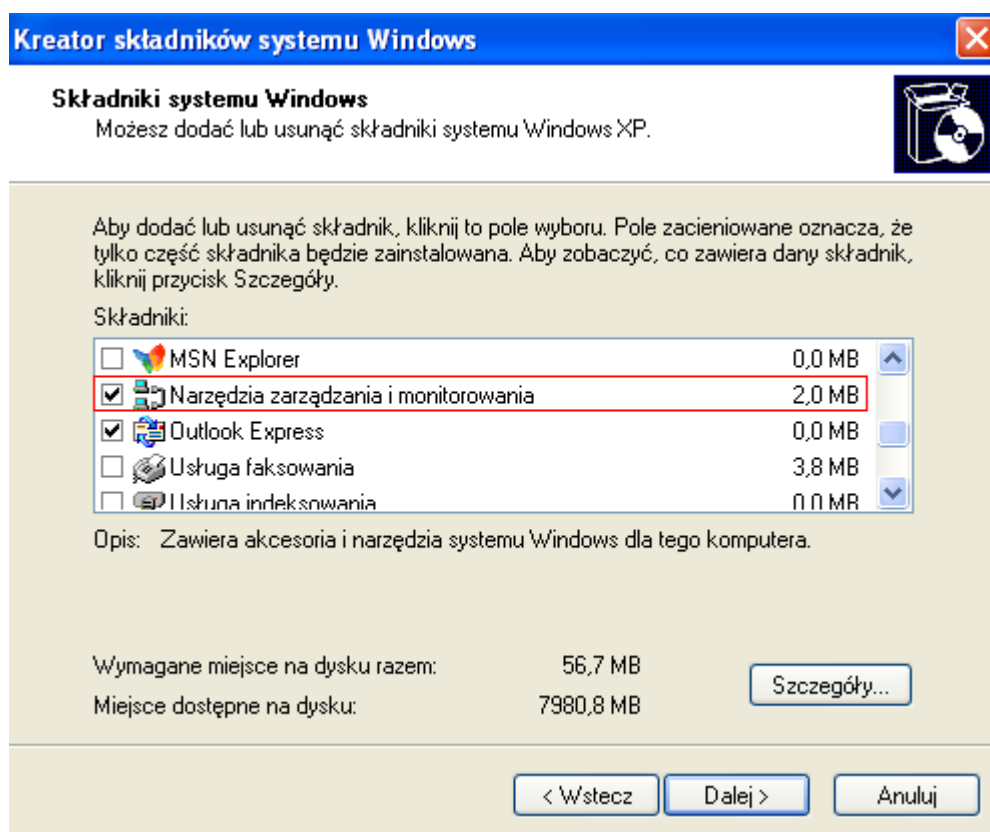
Kontrola dostępu – w SNMPv3 występuje kontrola dostępu oparta na widokach. Dzięki temu można ustawić do jakich informacji mają dostęp poszczególni użytkownicy. Informacje o polityce dostępu i uprawnieniach są przechowywane w lokalnej bazie danych konfiguracyjnych (ang. Local Configuration Datastore – LCD).

1.3 Przebieg ćwiczenia

Ćwiczenia będą wykonywane na bezpłatnej wersji programu iReasoning MIB Browser. Poniższa konfiguracja jest przedstawiona dla Windowsa XP.

1.3.1 Uruchom i skonfiguruj protokół SNMP.

1. W tym celu uruchom kolejno **Panel sterowania** → **dodaj lub usuń programy** → **dodaj/usuń składniki systemu Windows**.
2. W nowo otwartym oknie (Rys. 1) sprawdź czy jest zaznaczone pole wyboru przy składniku systemu Windows – **Narzędzia zarządzania i monitorowania**.
3. Jeśli nie, to zaznacz i kliknij przycisk dalej.

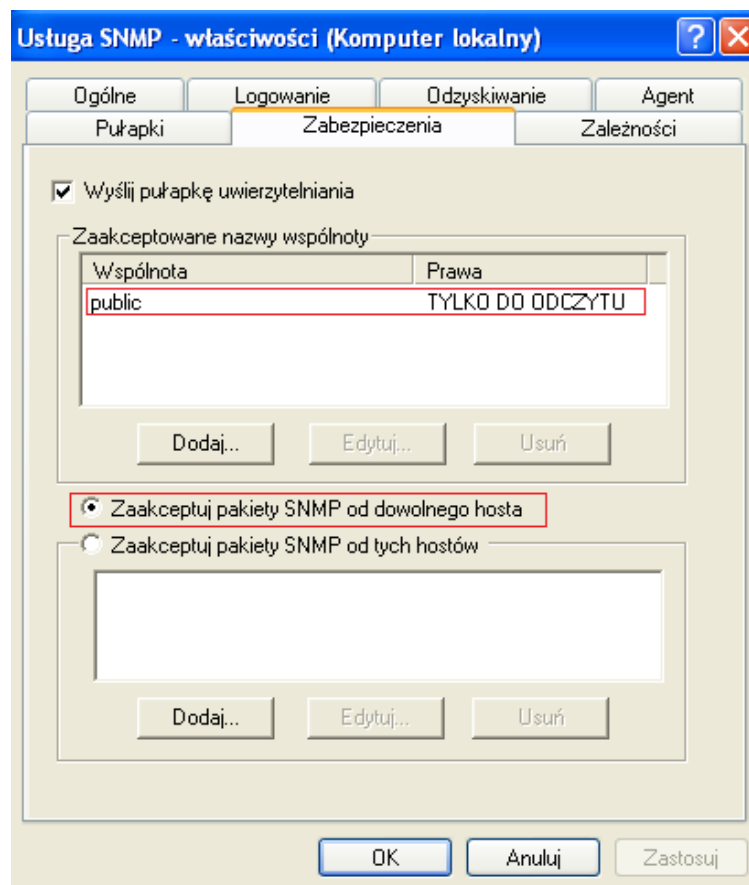


Rys. 1. Składniki systemu Windows

4. Następnie wejdź w **Panel sterowania** → **narzędzia administracyjne** → **zarządzanie komputerem** → **usługi i aplikacje** → **usługi**.
5. Z listy wybierz **usługę SNMP** poprzez dwukrotne kliknięcie. Pojawi się okno takie jak ilustruje Rys. 3.
6. Przejdź na zakładkę **zabezpieczenia** i sprawdź czy w okienku **zaakceptowane nazwy wspólnoty** jest ustawiona wspólnota o nazwie **public** na prawach **tylko do odczytu**.
7. Jeśli nie, to poprzez przycisk **dodaj** utwórz taką wspólnotę.
8. Powinna być również zaznaczona opcja **zaakceptuj pakiety SNMP od dowolnego hosta**.
9. Wyłącz zaporę systemu Windows, aby dochodziły komunikaty SNMP. Aby to zrobić kliknij na pasku narzędzi w miejscu zaznaczonym na Rys. 2.



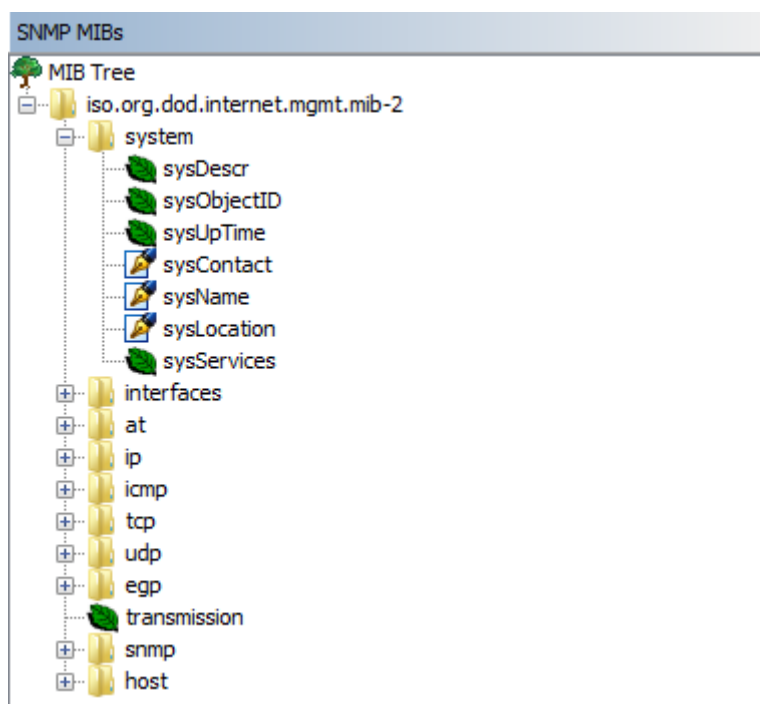
Rys. 2. Zapora systemu Windows



Rys. 3. Konfiguracja protokołu SNMP

1.3.2 Uruchom program iReasoning MIB Browser.

1.3.3 Zapoznaj się ze strukturą bazy MIB.



Rys. 4. Struktura bazy MIB

Po zaznaczeniu danego obiektu możesz poniżej odczytać informacje na jego temat. Przedstawia to Rys. 5.

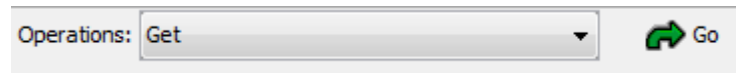
Name	sysUpTime
OID	.1.3.6.1.2.1.1.3
MIB	RFC1213-MIB
Syntax	TimeTicks
Access	read-only
Status	mandatory
DefVal	
Indexes	
Descr	The time (in hundredths of a second) since the network management portion of the system was last re-initialized.

Rys. 5. Informacje o danym obiekcie

1.3.4 Odczytaj informacje z grupy system.

1. W okienku **address** wpisz adres IP lub nazwę swojego komputera.
2. Następnie zaznacz dowolny obiekt z grupy **system** i z listy rozwijanej **operations** (Rys. 6) wybierz **Get**.

3. Wciśnij przycisk **Go**.
4. Wypróbuj też działanie operacji **GetNext** oraz **GetBulk**.



Rys. 6. Lista operacji

1.3.5 Działanie operacji Set.

1. Wyświetl obiekt **sysName**.
2. Spróbuj użyć operacji **Set** na tym obiekcie.
3. Jeśli nie działa, to uruchom **panel sterowania** → **narzędzia administracyjne** → **zarządzanie komputerem** → **usługi i aplikacje** → **usługi**.
4. Z listy wybierz usługę **SNMP**.
5. Na karcie **zabezpieczenia** zaznacz wspólnotę **public**, naciśnij przycisk **edytuj** i ustaw **prawa wspólnoty** na **odczyt zapis**.
6. Nie zamykając okna powrót do programu iReasoning MIB Browser i ponownie spróbuj użyć operacji **Set** na obiekcie **sysName**.
7. Jeśli operacja się powiodła, to wyświetl po raz drugi obiekt **sysName**, aby przekonać się, że nazwa uległa zmianie, tak jak na Rys. 7.
8. Teraz ponownie ustaw **prawa wspólnoty** na **tylko do odczytu**, aby wyeliminować możliwość zdalnej zmiany wartości.

Result Table			
Name/OID	Value	Type	IP:Port
sysName.0	Lenovo-Komputer12	OctetString	172.16.0.2:161
sysName.0	Lenovo-Komputer	OctetString	172.16.0.2:161

Rys. 7. Przykład działania operacji Set

1.3.6 Rozwiń grupę interfaces.

Całą tabelę interfejsów możesz wyświetlić zaznaczając obiekt **ifTable** i wykonując operację **Table View**. Grupę **interfaces** możesz natomiast przejrzeć wykonując operację **Get Subtree** na zaznaczonej grupie **interfaces**.

1.3.7 Działaj w parze z osobą przy drugim stanowisku komputerowym.

1. W polu **address** wpisz adres ip sąsiada.
2. Uruchom analizator **Wireshark**.
3. Rozpocznij rejestrację pakietów.
4. Filtruj ruch **SNMP**.

1.3.8 Pobierz jakąś wartość z drugiego komputera (np. sysName) za pomocą operacji Get.

W **Wiresharku** (Rys. 8) sprawdź jakie pola w PDU umieszcza jednostka wysyłająca i odbierająca.

Filter: snmp		Expression...		Clear	Apply	
No.	Time	Source	Destination	Protocol	Length	Info
33720	3080.382143	172.16.0.3	172.16.0.2	SNMP	250	get-response 1.3.6.1.2.1.25.4.2.1.1
33721	3080.382963	172.16.0.2	172.16.0.3	SNMP	199	get-next-request 1.3.6.1.2.1.25.4.2
33722	3080.388289	172.16.0.3	172.16.0.2	SNMP	230	get-response 1.3.6.1.2.1.25.4.2.1.1
33723	3080.388752	172.16.0.2	172.16.0.3	SNMP	199	get-next-request 1.3.6.1.2.1.25.4.2
33724	3080.391600	172.16.0.3	172.16.0.2	SNMP	218	get-response 1.3.6.1.2.1.25.4.2.1.2
65384	6449.257557	172.16.0.2	172.16.0.3	SNMP	85	get-request 1.3.6.1.2.1.1.5.0
65385	6449.333310	172.16.0.3	172.16.0.2	SNMP	97	get-response 1.3.6.1.2.1.1.5.0
65396	6451.809564	172.16.0.2	172.16.0.3	SNMP	85	get-next-request 1.3.6.1.2.1.1.5.0
65397	6451.814214	172.16.0.3	172.16.0.2	SNMP	85	get-response 1.3.6.1.2.1.1.6.0
65511	6492.852400	172.16.0.2	172.16.0.3	SNMP	85	get-request 1.3.6.1.2.1.1.5.0
65512	6492.855156	172.16.0.3	172.16.0.2	SNMP	97	get-response 1.3.6.1.2.1.1.5.0
65519	6495.183471	172.16.0.2	172.16.0.3	SNMP	85	get-request 1.3.6.1.2.1.1.5.0
65520	6495.186362	172.16.0.3	172.16.0.2	SNMP	97	get-response 1.3.6.1.2.1.1.5.0
65524	6497.017716	172.16.0.2	172.16.0.3	SNMP	85	get-request 1.3.6.1.2.1.1.5.0
65525	6497.021133	172.16.0.3	172.16.0.2	SNMP	97	get-response 1.3.6.1.2.1.1.5.0

Internet Protocol Version 4, Src: 172.16.0.2 (172.16.0.2), Dst: 172.16.0.3 (172.16.0.3)

User Datagram Protocol, Src Port: 59994 (59994), Dst Port: snmp (161)

Simple Network Management Protocol

version: version-1 (0)
community: public

data: get-request (0)

get-request

request-id: 504590296
error-status: noError (0)
error-index: 0

variable-bindings: 1 item

1.3.6.1.2.1.1.5.0: value (Null)
object Name: 1.3.6.1.2.1.1.5.0 (iso.3.6.1.2.1.1.5.0)
value (Null)

0000 78 92 9c 2a f5 60 00 26 82 9b f8 99 08 00 45 00 x..*.`.&E.
0010 00 47 56 f1 00 00 80 11 8b 8f ac 10 00 02 ac 10 .GV.....
0020 00 03 ea 5a 00 a1 00 33 04 2c 30 29 02 01 00 04 ...Z...3 ,0)....
0030 06 70 75 62 6c 69 63 a0 1c 02 04 1e 13 6f d8 02 .public.o..
0040 01 00 02 01 00 30 0e 30 0c 06 08 2b 06 01 02 010.0+....
0050 01 05 00 05 00

Rys. 8. Format jednostki GetRequest-PDU

1.3.9 Zaobserwuj w analizatorze Wireshark czy w jednostce typu **GetResponse** pojawiają się jakieś błędy, gdy próbujemy odczytać np. całą tabelę za pomocą polecenia **Get**.

1.3.10 Porównaj w Wiresharku działanie poleceń **Get** i **GetNext**.

Zwróć uwagę, że w przypadku PDU **GetRequest** każda zmienna w liście **variable-bindings** odnosi się do instancji obiektu, której wartość ma być odesłana. Natomiast przy PDU **GetNextRequest** dla każdej wymienionej zmiennej w odpowiedzi otrzymamy wartość tej instancji obiektu, która jest następną po podanej.

1.3.11 Sprawdź pole **variablebindings** w przypadku polecenia **GetBulk**. Zwróć uwagę, jakie zmienne przychodzą w odpowiedzi (Rys. 9).

71206	8221.710614	172.16.0.2	172.16.0.3	SNMP	85	getBulkRequest	1.3.6.1.2.1.1.1.0
71207	8221.714031	172.16.0.3	172.16.0.2	SNMP	252	get-response	1.3.6.1.2.1.1.2.0 1.


```

community: public
data: get-response (2)
  get-response
    request-id: 504590317
    error-status: noError (0)
    error-index: 0
    variable-bindings: 10 items
      1.3.6.1.2.1.1.2.0: 1.3.6.1.4.1.311.1.1.3.1.1 (iso.3.6.1.4.1.311.1.1.3.1.1)
        Object Name: 1.3.6.1.2.1.1.2.0 (iso.3.6.1.2.1.1.2.0)
        Value (OID): 1.3.6.1.4.1.311.1.1.3.1.1 (iso.3.6.1.4.1.311.1.1.3.1.1)
      1.3.6.1.2.1.1.3.0: 691833
        Object Name: 1.3.6.1.2.1.1.3.0 (iso.3.6.1.2.1.1.3.0)
        Value (Timeticks): 691833
      1.3.6.1.2.1.1.4.0: <MISSING>
        Object Name: 1.3.6.1.2.1.1.4.0 (iso.3.6.1.2.1.1.4.0)
        Value (OctetString): <MISSING>
      1.3.6.1.2.1.1.5.0: 656c612d4b6f6d7075746572
        Object Name: 1.3.6.1.2.1.1.5.0 (iso.3.6.1.2.1.1.5.0)
        Value (OctetString): 656c612d4b6f6d7075746572
      1.3.6.1.2.1.1.6.0: <MISSING>
        Object Name: 1.3.6.1.2.1.1.6.0 (iso.3.6.1.2.1.1.6.0)
  
```

Rys. 9. Format jednostki Response-PDU

1.3.12 Pułapki

1. W programie **iReasoning MIB Browser** ustaw odbieranie pułapek za pomocą **Tools** → **Trap Receiver**. Otworzy się okno jak na Rys. 10.
2. Następnie posługując się **Tools** → **Trap Sender** (Rys. 11) wyślij różne rodzaje pułapek (zakładka **Generic**) do drugiego komputera z pary.
3. Zaobserwuj też w programie **Wireshark** jak wygląda struktura pułapki.

Trap Receiver		
Operations Tools		
Description	Source	Time
egpNeighborLoss	172.16.0.6	2013-07-17 14:01:54
egpNeighborLoss	172.16.0.6	2013-07-17 14:01:47
egpNeighborLoss	172.16.0.6	2013-07-17 14:01:47
egpNeighborLoss	172.16.0.3	2013-07-17 13:52:35
linkDown	172.16.0.3	2013-07-17 13:52:31
coldStart	172.16.0.3	2013-07-17 13:52:26
warmStart	172.16.0.3	2013-07-17 13:51:00
coldStart	172.16.0.3	2013-07-17 13:50:55
linkUp	172.16.0.3	2013-07-17 13:49:44
linkDown	172.16.0.3	2013-07-17 13:47:20
warmStart	172.16.0.3	2013-07-17 13:47:16
coldStart	172.16.0.3	2013-07-17 13:47:07

Rys. 10. Odebrane pulapki

Trap Sender

IP Address: 172.16.0.3 Port: 162

Number of Retries: 1 Timeout(sec): 2

Parameters:

Type: SNMPv1 Trap Community: public

Generic: ColdStart Specific: 0

Enterprise OID: Timestamp (sec): 0

Variable Bindings (optional):

OID/Name	Value	Type

Add

Modify

Delete

Suffix

Send Trap

Rys. 11. Wysylanie pulapek

4. Na jednym komputerze z pary zmień w usłudze **SNMP** nazwę wspólnoty z **public** na dowolną inną.
5. Upewnij się czy jest zaznaczona opcja „**Wyślij pułapkę uwierzytelnienia**”.
6. Na tym samym sprzęcie w zakładce „**Pułapki**” usługi SNMP ustaw nazwę społeczności **public** oraz jako miejsce docelowe pułapek wpisz adres IP drugiego komputera z pary.
7. Teraz na drugim hoście użyj polecenia **Get**, aby odczytać jakąś wartość z pierwszego urządzenia.
8. Sprawdź czy została odebrana pułapka uwierzytelnienia.

1.3.13 Poddzewo private bazy MIB

1. Do poddrzewa **private** wejdź wpisując ręcznie odpowiednie **OID**.
2. Wpisz **.1.3.6.1.4** i za pomocą operacji **Walk** lub **GetSubtree** przeanalizuj jakie informacje są zawarte w wynikach.

1.4 Sprawozdanie i wnioski

Studenci pracują przy osobnych stanowiskach komputerowych, ale dobrane pary współdziałają ze sobą. Poszczególne zalecane ćwiczenia laboranci wykonują samodzielnie lub przy współpracy. Duety przygotowują wspólne sprawozdanie uwzględniając wyniki uzyskane w laboratorium. Jednakże wnioski końcowe powinny być opracowane indywidualnie.

Opracował: Piotr Łękawa