PRZEGLĄD TELEINFORMATYCZNY
NR 1-2, 2014

Wybrane przypadki enumeracji systemu Windows Server 2012

Zbigniew SUSKI

Instytut Teleinformatyki i Automatyki WAT,
ul. Kaliskiego 2, 00-908 Warszawa
z.suski@ita.wat.edu.pl

STRESZCZENIE: W artykule przedstawiono wybrane zagadnienia dotyczące enumeracji systemu Windows Server 2012. Zaprezentowano przegląd literatury w tym zakresie, opisano zbudowane dla potrzeb eksperymentów środowisko badawcze, oraz przedstawiono najważniejsze cechy interfejsu NetBIOS oraz protokołów NetBT i CIFS/SMB, które wykorzystują ten interfejs. Zasadnicza część opracowania zawiera opis wybranych eksperymentów dotyczących enumeracji systemu Windows Server 2012 oraz omówienie uzyskanych wyników.

SŁOWA KLUCZOWE: bezpieczeństwo, systemy Windows, testy penetracyjne, enumeracja.

1. Wstęp

Słowo enumeracja pochodzi od łacińskiego słowa *enumeratio* i oznacza wyliczenie, wyszczególnienie, wymienienie [1]. Słowo to wykorzystywane jest w różnych kontekstach i nabiera wówczas różnych znaczeń. Przykładowo w teorii literatury oznacza charakterystyczny dla baroku środek stylistyczny polegający na wymienianiu w tekście kolejnych elementów pewnej całości, służący zwróceniu uwagi na prezentowane treści, wzmocnieniu znaczenia wypowiedzi. W informatyce może oznaczać m.in. zestaw nazwanych stałych liczb całkowitych [2] lub proces używany przez stos jądra sterownika USB, związany z wykrywaniem obecności urządzeń USB [3].

Niniejsze opracowanie dotyczy bezpieczeństwa systemów informatycznych i w tym obszarze wiedzy enumeracją nazywamy proces wyszukiwania informacji o zasobach systemu [4]. Zdobywane informacje dotyczą zasobów sieciowych i ich udostępniania, identyfikatorów kont i grup użytkowników, zainstalowanych aplikacji. Niektórzy autorzy do celów

enumeracji zaliczają również identyfikację systemu operacyjnego (*fingerprinting*). Nie jest to jednak ogólnie uznane podejście do zagadnień enumeracji i w niniejszym opracowaniu nie zostanie uwzględnione.

Duża część technik enumeracji jest skuteczna tylko w stosunku do określonego systemu operacyjnego lub rodziny systemów operacyjnych (np. MS Windows). Wobec tego ta faza uzyskiwania informacji o systemie powinna być poprzedzona właśnie wspomnianą identyfikacją systemu operacyjnego.

Enumeracja jest jednym z etapów działań realizowanych przez intruza, stawiającego sobie za cel uzyskanie jak największej ilości informacji o interesującym go systemie, aby w dalszej kolejności dokonać destrukcyjnego ataku. Powinna być wobec tego również uwzględniona podczas realizacji testu penetracyjnego. Wiedza o tym, jakich informacji może poszukiwać intruz oraz w jaki sposób nasz system może je udostępniać, pomoże w usunięciu tych luk w zabezpieczeniach.

W roku 1999 ukazało się pierwsze wydanie książki *Hacking Exposed* [4]. Jest to prawdopodobnie pierwsza publikacja, w której w miarę dokładnie przedstawiono przykłady enumeracji systemów Windows. Książka zdobyła ogromną popularność na rynku. W sumie pojawiło się 7 wydań. Ostatnie w 2012 roku [5]. Do 2012 roku sprzedano przeszło 600 000 egzemplarzy. Książka została przetłumaczona na 30 języków[1]. Stuart McClure prowadzi również związaną z tą książką stronę internetową[2]. W każdym wydaniu swojej książki, rozdział trzeci autorzy poświęcali enumeracji. Jednak zmiany obserwowane w kolejnych wydaniach, nie były znaczące.

W roku 2001, Joel Scambray i Stuart McClure wydali książkę poświęconą bezpieczeństwu systemu Windows 2000 [6]. W niej również umieszczony został rozdział dotyczący enumeracji, tym razem ograniczonej do systemu Windows 2000. Książka doczekała się trzech wydań, ostatnie w roku 2008 [7]. Jest to pozycja, w której znaleźć można najwięcej informacji dotyczących enumeracji systemów Windows. W obu seriach wydawniczych nie znajdziemy jednak żadnej informacji o warunkach, w jakich uzyskano prezentowane wyniki.

Przez ostatnie siedem lat na rynku wydawniczym nie ukazała się żadna pozycja, która wprowadzałaby istotne zmiany w naszej wiedzy dotyczącej enumeracji systemów Windows. Wyszukiwanie stron, na których można by było znaleźć coś istotnie nowego w zakresie tego zagadnienia – nie daje rezultatu. W nowych publikacjach dotyczących testów penetracyjnych, enumeracja jest traktowana po macoszemu, często sprowadzana do pozyskiwania banerów (*banner grabbing*) lub nie wychodzi poza zagadnienia przedstawione w prezentowanych wcześniej publikacjach [10]. Jedynie w starszych

[1] W Polsce przetłumaczono i opublikowano wydanie pierwsze (pod tytułem *Hakerzy cała prawda*) oraz wydanie piąte (pod tytułem *Hacking zdemaskowany*).
[2] http://www.hackingexposed.com/

publikacjach można, co nieco znaleźć [9]. Pojawia się wobec tego pytanie: czy jest już tak dobrze, że temat nie budzi zainteresowania? A może przez tych kilka lat nic się nie zmieniło – nie ma postępu i wobec tego nie ma, o czym pisać.

To właśnie stanowiło inspirację przeprowadzenia badań dotyczących zagadnień enumeracji najnowszej wersji serwerowej systemów firmy Microsoft –Windows Server 2012. Pierwsze wyniki przedstawiono w niniejszym opracowaniu. Pozostałe zostaną zamieszczone w kolejnych publikacjach.

2. Środowisko badawcze

Środowisko badawcze zostało zbudowane z wykorzystaniem pakietu VMware Workstation 11 [11]. W pierwszej fazie eksperymentów wykorzystano trzy maszyny wirtualne z systemem Windows Server 2012. Ich najważniejsze parametry, mające wpływ na uzyskane wyniki, zamieszczono w Tab. 1.

Tab. 1. Specyfikacja wykorzystywanych maszyn wirtualnych

Charakterystyka	Nazwa maszyny		
	SECINT	SECSTD	SECHI
Przeznaczenie	Maszyna intruza realizującego enumerację	Maszyna podlegająca enumeracji	Maszyna podlegająca enumeracji
Adres IP	172.16.100.3	172.16.100.1	172.16.100.4
Zapora sieciowa	Wyłączona	Wyłączona	Włączona (konfiguracja domyślna)
Hasło administratora	Password2	Password1	Password1
Login/hasło intruza1	Intruz/Password1	Intruz/Password1	Intruz/Password1
Login/hasło intruza 2	Tester/Password3	brak	brak
Uwagi	Na maszynach podlegających enumeracji SID systemu ustawiono inny niż na maszynie intruza		

Maszyna SECINT pełniła rolę maszyny intruza dokonującego enumeracji. Pozostałe maszyny podlegały enumeracji. Zastosowano konfiguracje domyślne, uzyskiwane podczas przebiegu typowej instalacji, bez wprowadzania dodatkowych komponentów. Na maszynie SECSTD wyłączona została zapora sieciowa. Na maszynie SECHI pozostała ona włączona, w konfiguracji uzyskanej podczas instalowania systemu.

Hasło konta administratora na maszynie SECINT miało inną wartość niż hasła kont administratorów na pozostałych maszynach. W ten sposób

zamodelowano brak znajomości przez intruza, hasła administratora na maszynach enumerowanych.

Podobnie identyfikator zabezpieczeń SID (*Security Identifier*) systemu SECINT miał inną wartość niż identyfikatory na pozostałych maszynach. W ten sposób zamodelowano unikalność SID na różnych komputerach w sieci. Brak tej unikalności mógłby mieć wpływ na uzyskiwane wyniki.

Brak zróżnicowania wartości SID i haseł administratorów na maszynach SECSTD i SECHI, nie ma żadnego znaczenia dla przebiegu i wyników przeprowadzonych eksperymentów. Systemy te nie współpracują ze sobą, tzn. nie wymieniają żadnych danych, istotnych z punktu widzenia eksperymentów.

Ostatnim czynnikiem wziętym pod uwagę podczas opracowywania środowiska badawczego, były parametry konta użytkownika realizującego enumerację zdalnego komputera. Należało tu wziąć pod uwagę pięć przypadków:

a) intruz zdobył login i hasło nieuważnego użytkownika komputera enumerowanego[3],
b) intruz nie posiada żadnej wiedzy odnośnie kont dostępnych na systemie podlegającym enumeracji i próbuje realizować enumerację zdalną wykorzystując swoje lokalne konto bez uprawnień administracyjnych,
c) intruz nie posiada żadnej wiedzy odnośnie kont dostępnych na systemie podlegającym enumeracji i próbuje realizować enumerację anonimowo,
d) intruz zna login i hasło wbudowanego konta administratora,
e) intruz „wszczepił" do systemu enumerowanego, poprzez odpowiedni *malware*, konto w grupie administratorów.

W pierwszej fazie badań wykorzystano wariant a). Mogłoby się wydawać, że jest to wariant nierealny, niemający zastosowania w rzeczywistości. Okazuje się jednak, że u sporej grupy użytkowników obserwuje się tendencję do wybierania haseł łatwych do odgadnięcia przez intruza. Teza taka pojawiła się w roku 1990, w tzw. raporcie Kleina [12]. Aktualnie potwierdzają to krótkie notatki publikowane na różnych stronach WWW[4]. Przedstawiają one wyniki

[3] Zdobyte konto należy do użytkownika, który nie posiada żadnych specjalnych przywilejów, a zwłaszcza nie należy do żadnej z grup administracyjnych.

[4] http://www.benchmark.pl/aktualnosci/Jesli_twoje_haslo_to_123456_-_zmien_je-26351.html
http://tech.wp.pl/kat,1009785,title,Oto-najpopularniejsze-hasla-uzytkownikow-Adobecom,wid,16207123,wiadomosc.html
http://www.chip.pl/news/bezpieczenstwo/luki-bezpieczenstwa/2014/10/do-sieci-wyciekly-hasla-uzytkownikow-dropboxa
http://www.chip.pl/news/bezpieczenstwo/wirusy/2014/05/apple-ma-nowy-problem-wyciek-hasel-uzytkownikow

badań jakości haseł wykorzystywanych przez użytkowników w różnych środowiskach. Wynika z nich np., że od lat najbardziej popularnym hasłem jest ciąg znaków „123456". Skutkiem jest dość duża skuteczność słownikowego lub hybrydowego ataku na hasła.

W badaniach wykorzystywane było konto INTRUZ, które potraktowano, jako reprezentanta dla omawianego przypadku. Zostało ono założone we wszystkich systemach środowiska badawczego. Dodatkowo wykorzystywano również konto TESTER. Konto to reprezentowało użytkownika, który nie ma rozeznania odnośnie kont rezydujących na komputerze podlegającym enumeracji. Jego użycie pozwalało na porównywanie wyników możliwych do osiągnięcia w przypadkach a) oraz b).

W badaniach, których wyniki przedstawiono w niniejszym opracowaniu, nie wzięto pod uwagę pozostałych wariantów. Zostaną one wykorzystane w dalszych badaniach.

3. NetBIOS, NetBT, CIFS/SMB

NetBIOS (***Net****work* ***B****asic* ***I****nput/****O****utput* ***S****ystem*) to mechanizm zaprojektowany we wczesnych latach 80-tych przez firmę IBM. Zapewnia podstawowy interfejs połączeń pomiędzy aplikacjami na różnych komputerach znajdujących się w tej samej sieci lokalnej. Umożliwia również współdzielenie danych.

NBT lub NetBT (*NetB**IOS*** *over* ***T****CP/IP*) to protokół sieciowy umożliwiający aplikacjom wykorzystującym API NetBIOS-u, komunikację w sieciach TCP/IP [13], [14].

NetBIOS dostarcza trzech odrębnych usług:

- usługi nazw, służącej rejestracji i przyznawania nazw (port 137/udp),
- usługi przekazywania datagramów w komunikacji bezpołączeniowej (port 138/udp),
- usługi sesji w komunikacji połączeniowej (port 139/tcp).

Wszystkie wymienione usługi zostały zaimplementowane w NBT. Protokół NBT był zawsze i nadal jest dostępny w systemach Windows. Począwszy od Windows 2000, dodatkowo wykorzystywany jest port 445/tcp.

Przestrzeń nazewnicza NetBIOS jest płaska, co oznacza, że każda nazwa musi być unikalna. Nazwa NetBIOS składa się z 16 bajtów. W nazwach zasobów

http://m.chip.pl/mobile/news/bezpieczenstwo/luki-bezpieczenstwa/2014/10/do-sieci-wyciekly-hasla-uzytkownikow-dropboxa/mobile_view

sieciowych Windows (np. usług), 15 bajtów jest traktowane, jako tzw. nazwa właściwa. Bajt 16 służy do określenia typu zasobu i jest określany mianem przyrostka NetBIOS.

Przykładowe przyrostki nazw NetBIOS zostały przedstawione w Tab. 2.

Tab. 2. Przykładowe przyrostki nazw NetBIOS

Nazwa	Przyrostek NetBIOS	Typ zasobu
<nazwa komputera>	00h	Usługa *Workstation*
<nazwa komputera>	20h	Usługa *Server*
<nazwa komputera>	03h	Usługa *Messenger*
<nazwa komputera>	06h	Usługa *RAS Server*
<nazwa domeny>	1Dh	Usługa *Master Browser*
<nazwa domeny>	00h	Domena lub grupa robocza

SMB (*Server Message Block*) jest protokołem umożliwiającym m.in. współdzielenie plików, drukarek, uwierzytelnienie w komunikacji międzyprocesowej, blokowanie plików i katalogów. **CIFS** (*Common Internet File System*) jest dialektem (jedną z wersji) SMB. W modelu sieciowym ISO są one umieszczane w warstwie 6 lub 7. W warstwie transportowej, oba protokoły najczęściej wykorzystują wspomniany wcześniej NBT. Nie jest to jednak rozwiązanie obowiązujące. Ma na celu zapewnić przede wszystkim tzw. kompatybilność wsteczną[5] systemów Windows.

Wymienione w niniejszym rozdziale mechanizmy były i są uważane za jedną z najważniejszych przyczyn „nadmiernej gadatliwości" systemów Windows, co skutkuje dość dużą łatwością pozyskiwania z nich informacji o zasobach.

4. Enumeracja za pomocą programu *nbtstat*

Program ***nbtstat*** jest wbudowanym narzędziem systemu Windows 2012, umożliwiającym przeglądanie tabeli nazw NetBIOS komputera. Na rys. 1 przedstawiono raport uzyskany podczas enumeracji systemu SECHI.

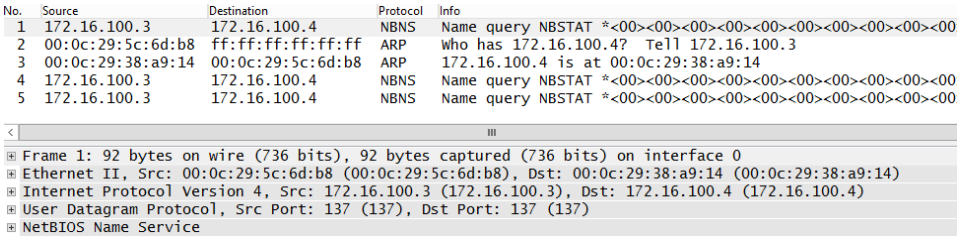
Jest to system chroniony zaporą sieciową (patrz Tab.1). Wobec tego, jak można się było spodziewać, żądanie danych zostało zignorowane. Doskonale obrazuje to ruch sieciowy przedstawiony na rys. 2. Podczas eksperymentu uzyskano pozytywną odpowiedź na wysłane żądanie ARP. Trzykrotne próby

[5] Zgodność funkcjonalna z poprzednimi, starszymi wersjami systemów. Dzięki temu możliwa jest współpraca nowych wersji systemów z wersjami starszymi.

nawiązania sesji na porcie 137/udp pozostały bez odpowiedzi. Zgodnie z opisem przedstawionym w rozdziale 2, próba enumeracji była przeprowadzona z komputera SECINT (172.16.100.3).

```
C:\Users\intruz>nbtstat -A 172.16.100.4

Ethernet:
Node IpAddress: [172.16.100.3] Scope Id: []

    Host not found.

C:\Users\intruz>
```

Rys. 1. Raport programu *nbtstat* uzyskany podczas enumeracji systemu SECHI



Rys. 2. Ruch sieciowy uzyskany podczas enumeracji systemu SECHI

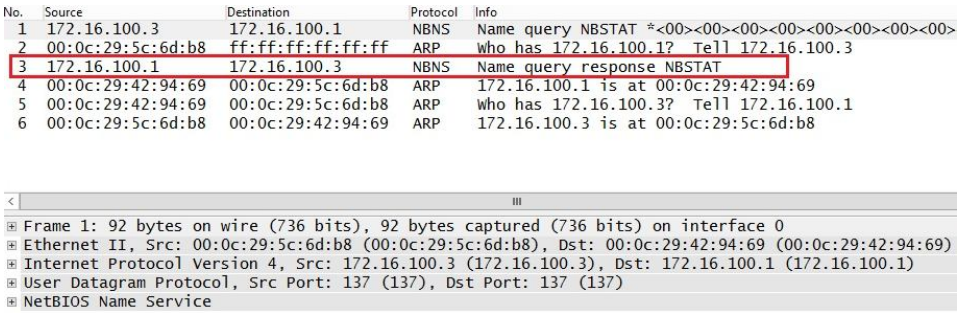
Kolejny eksperyment dotyczył systemu, w którym zapora sieciowa została wyłączona. Był to komputer SECSTD (172.16.100.1).

```
C:\Users\intruz>whoami
secint\intruz

C:\Users\intruz>nbtstat -A 172.16.100.1

Ethernet:
Node IpAddress: [172.16.100.3] Scope Id: []

            NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    WORKGROUP      <00>  GROUP        Registered
    SECSTD         <00>  UNIQUE       Registered
    SECSTD         <20>  UNIQUE       Registered

    MAC Address = 00-0C-29-42-94-69


C:\Users\intruz>_
```

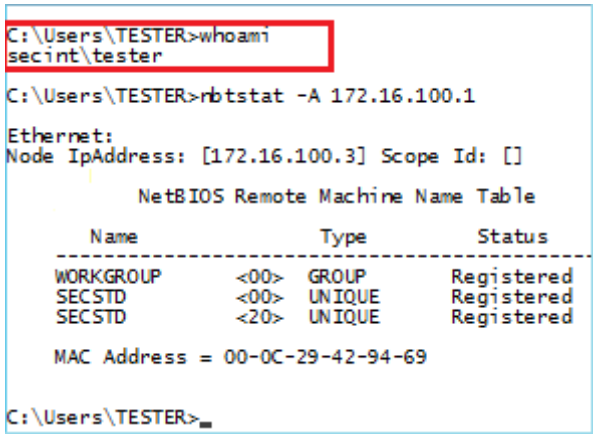
Rys. 3. Raport programu *nbtstat* uzyskany podczas enumeracji systemu SECSTD (z wykorzystaniem konta INTRUZ)

Na rys. 3 przedstawiono raport uzyskany podczas tego eksperymentu. Można z niego odczytać, że enumerowany system jest elementem domeny lub grupy roboczej o nazwie WORKGROUP, nosi nazwę SECSTD i uruchomione zostały na nim usługi *Server* i *Workstation*. Odczytać można również adres fizyczny (MAC) adaptera sieciowego. W raporcie zaznaczono wiersz uruchomienia polecenia ***whoami***, z którego wynika, że enumeracja była realizowana przy użyciu konta INTRUZ.

Obraz ruchu sieciowego uzyskany podczas tego eksperymentu przedstawiono na rys. 4. Zaznaczono na nim pakiet zawierający odpowiedź na wysłane żądanie. Nie zamieszczono wyników dogłębnej analizy tego pakietu, gdyż nie wnosi to żadnej dodatkowej informacji.



Rys. 4. Ruch sieciowy uzyskany podczas enumeracji za pomocą programu *nbtstat* systemu SECSTD

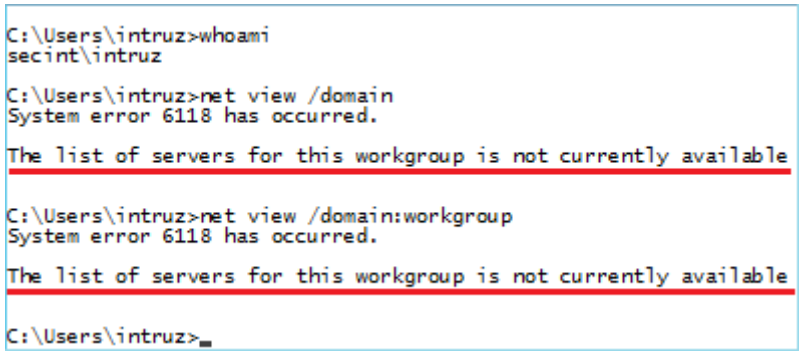


Rys. 5. Raport programu *nbtstat* uzyskany podczas enumeracji systemu SECSTD (z wykorzystaniem konta TESTER)

Wykorzystanie konta TESTER dało identyczne rezultaty. Wynika to z faktu, że w czasie dostępu do komputera zdalnego, nie było wymagane uwierzytelnienie klienta żądającego danych. Raport uzyskany podczas tego eksperymentu przedstawia rys. 5.

5. Enumeracja za pomocą programu *net view*

Program ***net view*** jest wbudowanym narzędziem systemu Windows 2012, umożliwiającym uzyskiwanie informacji odnośnie listy dostępnych domen, grup roboczych oraz funkcjonujących w nich komputerów. Dane te są dostarczane przez usługę *Computer Browser*. W domyślnej konfiguracji systemu Windows Server 2012 usługa ta jest wyłączona. Jak napisano w rozdziale 2, testowaniu podlegały domyślne konfiguracje systemu Windows Server 2012. Wobec tego próby enumeracji nie przyniosły rezultatu. Raporty uzyskane podczas tych prób przedstawiono na rys. 6.

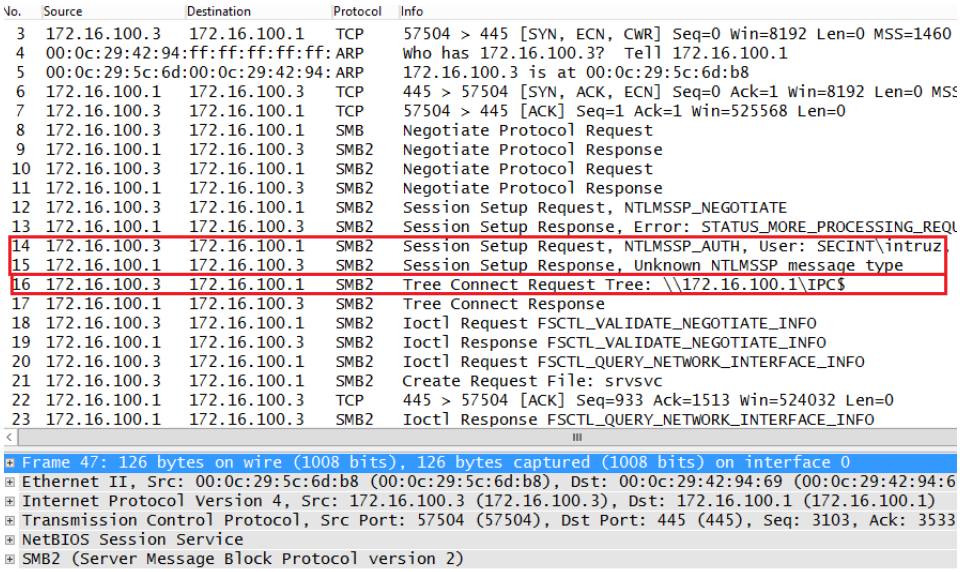


Rys. 6. Raporty programu *net view* uzyskane podczas enumeracji sieci środowiska badawczego

Specyfikacja programu ***net view*** przewiduje również możliwość uzyskania listy udziałów sieciowych udostępnionych na komputerze zdalnym. Raport takiego przypadku użycia przedstawia rys. 7. Jak można na nim zauważyć, wykrywane są nie tylko udziały udostępniane w trybie tradycyjnym (WAZNE_DANE_JAWNE), ale również udziały udostępniane, jako ukryte (BARDZO_WAZNE_UKRYTE_DANE$). Wykrywane są również udziały administracyjne, udostępniane automatycznie (ADMIN$, C$, E$), oraz udział stanowiący kanał komunikacji międzymaszynowej (IPC$).

```
C:\Users\intruz>whoami
secint\intruz

C:\Users\intruz>net view \\172.16.100.1 /all
Shared resources at \\172.16.100.1


Share name                  Type  Used as  Comment

-------------------------------------------------------------------------
ADMIN$                      Disk           Remote Admin
BARDZO_WAZNE_UKRYTE_DANE$   Disk
C$                          Disk           Default share
E$                          Disk           Default share
IPC$                        IPC            Remote IPC
WAZNE_DANE_JAWNE            Disk
The command completed successfully.


C:\Users\intruz>
```

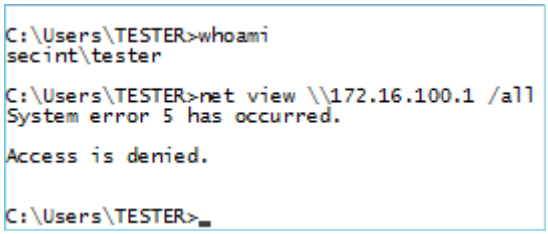
Rys. 7. Raport programu *net view* uzyskany podczas enumeracji systemu SECSTD (z wykorzystaniem konta INTRUZ)



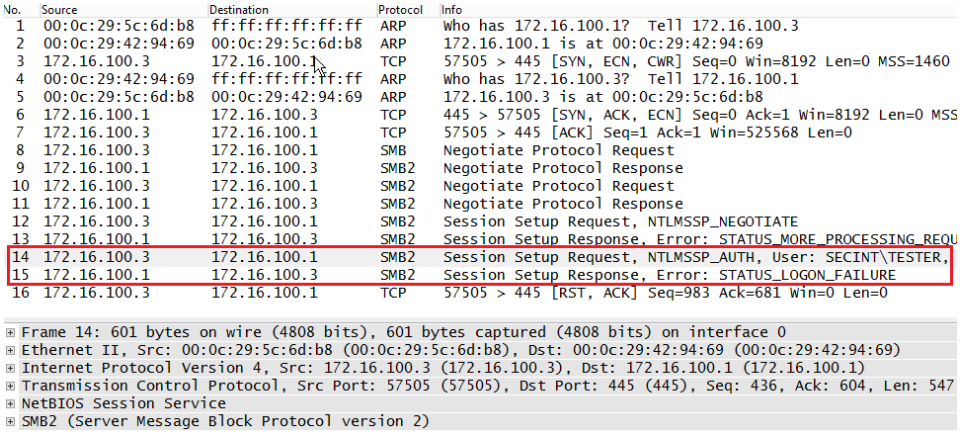
Rys. 8. Fragment ruchu sieciowego uzyskany podczas enumeracji za pomocą programu *net view* systemu SECSTD (z wykorzystaniem konta INTRUZ)

Obraz fragmentu ruchu sieciowego uzyskany podczas tego eksperymentu przedstawiono na rys. 8. Należy zwrócić uwagę na sekwencję nawiązywania połączenia na porcie 445 (pakiety 3, 6, 7), sekwencję związaną z uwierzytelnieniem (m.in. pakiet 14 i 15) oraz żądanie podłączenia do zasobu

komunikacji międzymaszynowej IPC$ (pakiet 16). Interesujący jest fakt, że mimo podania niewłaściwej nazwy domeny (podano domenę enumeratora SECINT a nie domenę hosta badanego SECSTD), uwierzytelnienie zakończyło się powodzeniem. Przyczyną jest stosowanie w fazie uwierzytelnienia, protokołu NTLM [15]. Przy zastosowaniu tego protokołu, nazwa użytkownika jest przesyłana otwartym tekstem, co oznacza, że łatwo jest dokonać enumeracji kont użytkowników poprzez podsłuchiwanie ruchu sieciowego. Mimo, że opisano już szereg podatności protokołu NTLM, w dalszym ciągu jest on powszechnie stosowany, nawet w najnowszych wersjach systemów Windows. Zwykle tłumaczy się to koniecznością zachowania kompatybilności wstecznej.



Rys. 9. Raport programu *net view* uzyskany podczas enumeracji systemu SECSTD (z wykorzystaniem konta TESTER)



Rys. 10. Ruch sieciowy uzyskany podczas enumeracji za pomocą programu *net view* systemu SECSTD (z wykorzystaniem konta TESTER)

W czasie badań zrealizowano również eksperyment, w którym

wykorzystano konto TESTER. Jak napisano w rozdziale 2, reprezentowało ono intruza, który nie posiada żadnej wiedzy odnośnie kont dostępnych na systemie podlegającym enumeracji i próbuje realizować enumerację zdalną wykorzystując swoje lokalne konto bez uprawnień administracyjnych.

Raport z takiego badania przedstawiono na rys. 9. Intruzowi nie udało się uzyskać oczekiwanych danych. Przyczyną jest odrzucenie żądania uwierzytelnienia. Można to stwierdzić na podstawie obrazu ruchu sieciowego zamieszczonego na rys. 10 (pakiet 14 i 15).

6. Enumeracja za pomocą programu *userinfo*

Timothy Mullen występujący w sieci pod pseudonimem *Hammer of God*[6] napisał program ***userinfo*** jako swoisty *proof of concept*. Jego celem, jak sam twierdzi, było pokazanie niespójności w implementacji mechanizmu związanego z ustawieniem rejestru *RestrictAnonymous* w systemach Windows. Ustawienie to miało być środkiem zabezpieczającym, uniemożliwiającym „wyciek" wrażliwych danych z systemu. Timothy Mullen wykorzystał w swoim programie funkcję *NetUserGetInfo*[7].

Na rys. 11 przedstawiono raport z przebiegu programu ***userinfo*** uruchomionego na koncie użytkownika INTRUZ.

Żądanie enumeracyjne było skierowane do komputera SECSTD (172.16.100.1) i dotyczyło konta lokalnego INTRUZ na tym komputerze. Jak widać pozyskano wiele informacji o tym koncie:

- opis (*Comment*),
- identyfikator użytkownika (*User ID*): RID=1001),
- identyfikator grupy (*Primary Grp*): 513- wbudowana grupa *Users*,
- datę i czas ostatniej zmiany hasła (*Password Age*),
- datę i czas ostatniego logowania (*LastLogon*),
- ilość logowań (*Num logons*),
- ścieżka dostępu (UNC) dostępu do profilu użytkownika (*Profile*),
- napęd logiczny, na którym zamapowano folder domowy (*Homedir drive*),
- ścieżka dostępu (UNC) dostępu do foldera domowego (*Home Dir*).

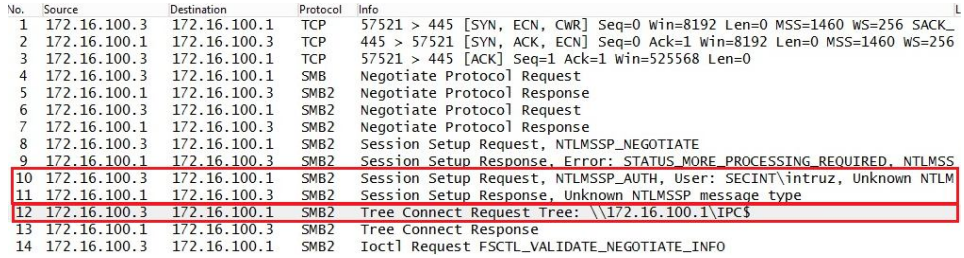
[6] www.hammerofgod.com
[7] https://msdn.microsoft.com/en-us/library/windows/desktop/aa370654%28v=vs.85%29

Rys. 11. Raport programu *userinfo* uzyskany podczas enumeracji systemu SECSTD (z wykorzystaniem konta INTRUZ)

Nie wszystkie dane umieszczone w raporcie przedstawionym na rys. 11 są poprawne. Wynika to m.in. z faktu, że program ***userinfo*** przeznaczony jest w zasadzie do pozyskiwania informacji o zadanym koncie z kontrolera domeny. W środowisku badawczym wykorzystywano tylko systemy autonomiczne, pracujące w grupie roboczej. Niektóre atrybuty kont użytkowników domenowych nie występują w przypadku kont lokalnych. Enumeracja w środowisku domenowym będzie przedmiotem osobnego opracowania.

Obraz fragmentu ruchu sieciowego uzyskany podczas tego eksperymentu

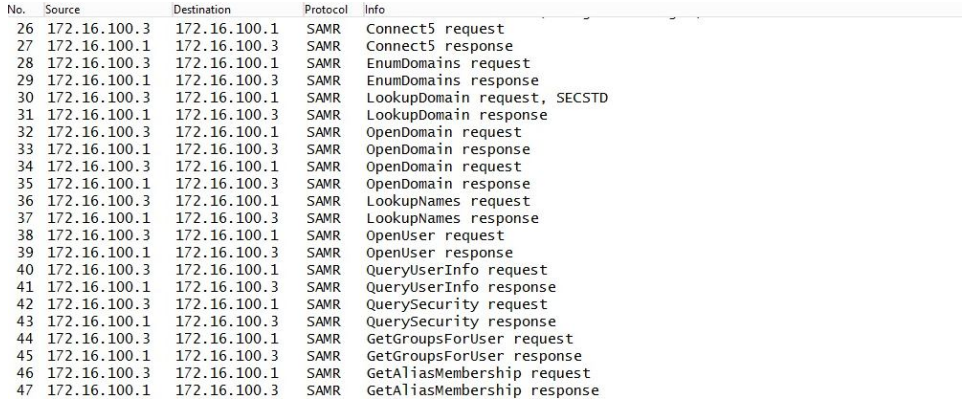
przedstawiono na rys. 12. Należy zwrócić uwagę na sekwencję nawiązywania połączenia na porcie 445 (pakiety 1÷3), sekwencję związaną z uwierzytelnieniem (m.in. pakiet 10 i 11) oraz żądanie podłączenia do zasobu komunikacji międzymaszynowej IPC$ (pakiet 12). Podobnie jak w wynikach eksperymentu przedstawionego na rys. 8, można zauważyć, że mimo podania niewłaściwej nazwy domeny (podano domenę enumeratora SECINT a nie domenę hosta badanego SECSTD), uwierzytelnienie zakończyło się powodzeniem. Wykorzystany został protokół NTLM.



No.	Source	Destination	Protocol	Info
1	172.16.100.3	172.16.100.1	TCP	57521 > 445 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_
2	172.16.100.1	172.16.100.3	TCP	445 > 57521 [SYN, ACK, ECN] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256
3	172.16.100.3	172.16.100.1	TCP	57521 > 445 [ACK] Seq=1 Ack=1 Win=525568 Len=0
4	172.16.100.3	172.16.100.1	SMB	Negotiate Protocol Request
5	172.16.100.1	172.16.100.3	SMB2	Negotiate Protocol Response
6	172.16.100.3	172.16.100.1	SMB2	Negotiate Protocol Request
7	172.16.100.1	172.16.100.3	SMB2	Negotiate Protocol Response
8	172.16.100.3	172.16.100.1	SMB2	Session Setup Request, NTLMSSP_NEGOTIATE
9	172.16.100.1	172.16.100.3	SMB2	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSS
10	172.16.100.3	172.16.100.1	SMB2	Session Setup Request, NTLMSSP_AUTH, User: SECINT\intruz, Unknown NTLM
11	172.16.100.1	172.16.100.3	SMB2	Session Setup Response, Unknown NTLMSSP message type
12	172.16.100.3	172.16.100.1	SMB2	Tree Connect Request Tree: \\172.16.100.1\IPC$
13	172.16.100.1	172.16.100.3	SMB2	Tree Connect Response
14	172.16.100.3	172.16.100.1	SMB2	Ioctl Request FSCTL_VALIDATE_NEGOTIATE_INFO

Rys. 12. Początkowy fragment ruchu sieciowego uzyskany podczas enumeracji za pomocą programu *userinfo* systemu SECSTD (z wykorzystaniem konta INTRUZ)

Obraz innego fragmentu ruchu sieciowego uzyskany podczas opisywanego eksperymentu przedstawiono na rys.13.



No.	Source	Destination	Protocol	Info
26	172.16.100.3	172.16.100.1	SAMR	Connect5 request
27	172.16.100.1	172.16.100.3	SAMR	Connect5 response
28	172.16.100.3	172.16.100.1	SAMR	EnumDomains request
29	172.16.100.1	172.16.100.3	SAMR	EnumDomains response
30	172.16.100.3	172.16.100.1	SAMR	LookupDomain request, SECSTD
31	172.16.100.1	172.16.100.3	SAMR	LookupDomain response
32	172.16.100.3	172.16.100.1	SAMR	OpenDomain request
33	172.16.100.1	172.16.100.3	SAMR	OpenDomain response
34	172.16.100.3	172.16.100.1	SAMR	OpenDomain request
35	172.16.100.1	172.16.100.3	SAMR	OpenDomain response
36	172.16.100.3	172.16.100.1	SAMR	LookupNames request
37	172.16.100.1	172.16.100.3	SAMR	LookupNames response
38	172.16.100.3	172.16.100.1	SAMR	OpenUser request
39	172.16.100.1	172.16.100.3	SAMR	OpenUser response
40	172.16.100.3	172.16.100.1	SAMR	QueryUserInfo request
41	172.16.100.1	172.16.100.3	SAMR	QueryUserInfo response
42	172.16.100.3	172.16.100.1	SAMR	QuerySecurity request
43	172.16.100.1	172.16.100.3	SAMR	QuerySecurity response
44	172.16.100.3	172.16.100.1	SAMR	GetGroupsForUser request
45	172.16.100.1	172.16.100.3	SAMR	GetGroupsForUser response
46	172.16.100.3	172.16.100.1	SAMR	GetAliasMembership request
47	172.16.100.1	172.16.100.3	SAMR	GetAliasMembership response

Rys. 13. Fragment ruchu sieciowego uzyskany podczas enumeracji za pomocą programu *userinfo* systemu SECSTD (z wykorzystaniem konta INTRUZ)

Jest to fragment pobierania szczegółowych danych dotyczących konta wskazanego w parametrach wywołania programu ***userinfo***. Jak można zauważyć wykorzystywany jest do tego protokół SAMR (*Security Account Manager*

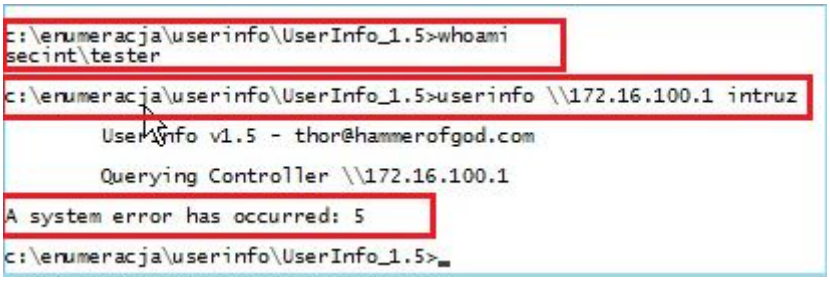
Remote Procedure Call) [16]. Jest on integralnym podsystemem służącym do wykonywania zdalnych operacji menedżera kont, takich jak zarządzanie i manipulowanie kontami użytkowników. Interfejs protokołu SAMR definiuje zdalne metody menedżera kont wywoływane przez klienta. Dostępna jest m.in. funkcja *SamConnect* służąca do łączenia się z bazą danych tego menedżera.

W zaleceniach dla implementatorów tego protokołu można znaleźć zapis, aby zwrócili oni szczególną uwagę na dane wrażliwe, takie jak hasła, które mogą być przesyłane otwartym tekstem. W zbiorze dostępnych funkcji są, bowiem również takie, które zapewniają ochronę kryptograficzną przesyłanych haseł.

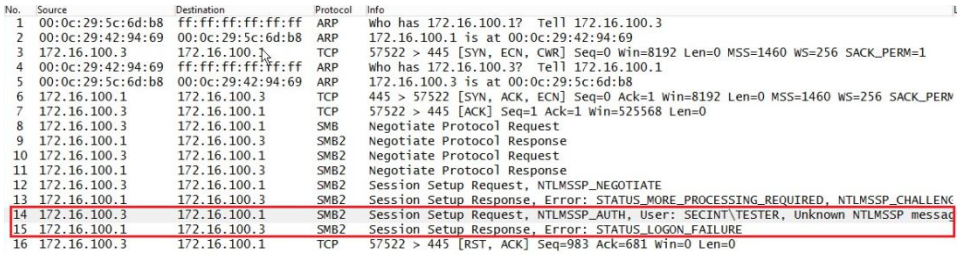
W trakcie badań dokonano również prób uzyskania informacji o innych kontach użytkowników systemu SECSTD. Podobnie jak w opisywanym eksperymencie wykorzystano konto INTRUZ. Jak napisano w rozdziale 2, konto INTRUZ reprezentuje napastnika, który zdobył login i hasło nieuważnego użytkownika komputera enumerowanego i wykorzystuje je do enumerowania zasobów tego komputera.

W czasie badań zrealizowano również eksperyment, w którym wykorzystano konto TESTER. Jak napisano w rozdziale 2, reprezentowało ono intruza, który nie posiada żadnej wiedzy odnośnie kont dostępnych na systemie podlegającym enumeracji i próbuje realizować enumerację zdalną wykorzystując swoje lokalne konto bez uprawnień administracyjnych.

Raport z takiego badania przedstawiono na rys. 14. Intruzowi nie udało się uzyskać oczekiwanych danych. Przyczyną jest odrzucenie żądania uwierzytelnienia. Można to stwierdzić na podstawie obrazu ruchu sieciowego zamieszczonego na rys. 15 (pakiet 14 i 15). Jak można zauważyć jest to efekt identyczny, jak w przypadku wykorzystania konta TESTER do enumeracji za pomocą programu ***net view***.



Rys. 14. Raport programu *userinfo* uzyskany podczas enumeracji systemu SECSTD (z wykorzystaniem konta TESTER)



No.	Source	Destination	Protocol	Info
1	00:0c:29:5c:6d:b8	ff:ff:ff:ff:ff:ff	ARP	Who has 172.16.100.1? Tell 172.16.100.3
2	00:0c:29:42:94:69	00:0c:29:5c:6d:b8	ARP	172.16.100.1 is at 00:0c:29:42:94:69
3	172.16.100.3	172.16.100.1	TCP	57522 > 445 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4	00:0c:29:42:94:69	ff:ff:ff:ff:ff:ff	ARP	Who has 172.16.100.3? Tell 172.16.100.1
5	00:0c:29:5c:6d:b8	00:0c:29:42:94:69	ARP	172.16.100.3 is at 00:0c:29:5c:6d:b8
6	172.16.100.1	172.16.100.3	TCP	445 > 57522 [SYN, ACK, ECN] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
7	172.16.100.3	172.16.100.1	TCP	57522 > 445 [ACK] Seq=1 Ack=1 Win=525568 Len=0
8	172.16.100.3	172.16.100.1	SMB	Negotiate Protocol Request
9	172.16.100.1	172.16.100.3	SMB2	Negotiate Protocol Response
10	172.16.100.3	172.16.100.1	SMB2	Negotiate Protocol Request
11	172.16.100.1	172.16.100.3	SMB2	Negotiate Protocol Response
12	172.16.100.3	172.16.100.1	SMB2	Session Setup Request, NTLMSSP_NEGOTIATE
13	172.16.100.1	172.16.100.3	SMB2	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENG
14	172.16.100.3	172.16.100.1	SMB2	Session Setup Request, NTLMSSP_AUTH, User: SECINT\TESTER, Unknown NTLMSSP messag
15	172.16.100.1	172.16.100.3	SMB2	Session Setup Response, Error: STATUS_LOGON_FAILURE
16	172.16.100.3	172.16.100.1	TCP	57522 > 445 [RST, ACK] Seq=983 Ack=681 Win=0 Len=0

Rys. 15. Ruch sieciowy uzyskany podczas enumeracji za pomocą programu *userinfo* systemu SECSTD (z wykorzystaniem konta TESTER)

7. Podsumowanie

W artykule przedstawiono wybrane, podstawowe techniki enumeracji systemu Windows Server 2012. Jak napisano w rozdziale wstępnym, inspirację przeprowadzenia badań dotyczących zagadnień enumeracji systemu Windows Server 2012 stanowiło stwierdzenie faktu, że przez ostatnie kilka lat na rynku wydawniczym nie ukazała się żadna pozycja, która wprowadzałaby istotne zmiany w naszej wiedzy dotyczącej enumeracji systemów Windows. Pojawiło się wobec tego pytanie: czy jest już tak dobrze, że temat nie budzi zainteresowania?. A może przez tych kilka lat nic się nie zmieniło – nie ma postępu i wobec tego nie ma, o czym pisać.

Jak wykazały przedstawione wyniki badań, odpowiedzi na postawione pytanie należy poszukiwać pomiędzy tymi skrajnościami. System Windows Server 2012, podobnie jak starsze wersje w dalszym ciągu jest podatny na działania enumeracyjne. Ze względu na brak specyfikacji środowisk, w których przeprowadzano badania dotyczące starszych systemów Windows, nie można dokonać wyczerpującego porównania. Nie jest to jednak chyba aż tak istotne. Istotne jest udzielenie odpowiedzi na pytanie dotyczące stanu zabezpieczeń nowego systemu, jakim jest Windows Server 2012. A z tym nie jest najlepiej. Udzielenie pełniejszej odpowiedzi na pytanie dotyczące bezpieczeństwa systemu Windows Server 2012 wymaga przeprowadzenia dalszych badań. W czasie eksperymentów należało wziąć pod uwagę pięć przypadków dotyczących kont wykorzystywanych w czasie enumeracji:

a) intruz zdobył login i hasło nieuważnego użytkownika komputera enumerowanego[8].
b) intruz nie posiada żadnej wiedzy odnośnie kont dostępnych na systemie podlegającym enumeracji i próbuje realizować enumerację zdalną

[8] Zdobyte konto należy do użytkownika, który nie posiada żadnych specjalnych przywilejów, a zwłaszcza nie należy do żadnej z grup administracyjnych.

wykorzystując swoje lokalne konto bez uprawnień administracyjnych,

c) intruz nie posiada żadnej wiedzy odnośnie kont dostępnych na systemie podlegającym enumeracji i próbuje realizować enumerację anonimowo,
d) intruz zna login i hasło wbudowanego konta administratora,
e) intruz „wszczepił" do systemu enumerowanego, poprzez odpowiedni *malware*, konto w grupie administratorów.

W pierwszej fazie badań, opisanej w niniejszym opracowaniu, wykorzystano wariant a) oraz b) jako wariant porównawczy. Jak stwierdzono wyżej, konieczne jest prowadzenie dalszych badań. Ich wyniki zostaną przedstawione w kolejnych publikacjach.

Literatura

[1] SOBOL E. (red.), *Słownik wyrazów obcych*, PWN, Warszawa, 1995.

[2] MIKOŁAJCZAK P., *Język C – podstawy programowania*, UMCS, Lublin, 2011.

[3] MIELCZAREK W., *USB – uniwersalny interfejs szeregowy*, Helion, Gliwice, 2005.

[4] SCAMBRAY J., MCCLURE S., KURTZ G., *Hacking Exposed: Network Security Secrets & Solutions*, McGraw Hill, Berkeley, 1999.

[5] SCAMBRAY J., MCCLURE S., KURTZ G., *Hacking Exposed: Network Security Secrets & Solutions 7th edition*, McGraw Hill, Berkeley, 2012.

[6] SCAMBRAY J., MCCLURE S., *Windows 2000 (Hacking Exposed)*, McGraw Hill, Berkeley, 2001.

[7] SCAMBRAY J., MCCLURE S., *Hacking Exposed Windows 3rd Edition*, McGraw Hill, Berkeley, 2008.

[8] ALLEN L., *Advanced Penetration Testing for Highly-Secured Environments*, Packt Publ. Ltd., Birmingham, 2012.

[9] KLEVINSKY T.J., LALIBERTE S., GUPTA A., *Security through Penetration Testing*, Addison Wesley, Birmingham, 2002.

[10] ENGEBRETSON P., *The Basics of Hacking and Penetration Testing*, Syngress Press, Waltham, 2011.

[11] VMWARE CORP., *Using VMware Workstation*, VMware Inc., Palo Alto, 2014.

[12] KLEIN D., V., *"Foilling the Cracker": A Survey of, and Improvements to, Password Security*, *In* Proceedings of the USENIX Second Security Workshop, Portland, Oregon, 1990.

[13] NETBIOS WORKING GROUP., *RFC 1001, Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Concepts and Methods*, 1987.

[14] NETBIOS WORKING GROUP., *RFC 1002, Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Detailed Specifications*, 1987.

[15] *[MS-NLMP] NT Lan Manager (NTLM) Authentication Protocol,* Microsoft Corp., 2014.

[16] *[MS-SAMR] Security Account Manager (SAM) Remote Protocol (Client-to-Server),* Microsoft Corp., 2014.

Enumeration selected cases of Windows Server 2012

ABSTRACT: The paper considers the issue of enumeration of Windows Server 2012. The paper gives a review of literature on the subject, describes the environment built for the needs of researches, presents the most important features of the NetBIOS interface, as well as NetBT and CIFS/SMB protocols that use this interface. The essential part of the paper contains a description of some experiments on the enumeration of Windows Server 2012 and a discussion of results.

KEYWORDS: security, Windows systems, penetration tests, enumeration

Praca wpłynęła do redakcji: 20.08.2014 r.