ВВМУ „НИКОЛА ЙОНКОВ ВАПЦАРОВ“
ФАКУЛТЕТ „ИНЖЕНЕРЕН“

Катедра „Информационни технологии“

инж. ДИМО БОЖИДАРОВ ДИМОВ

ИЗСЛЕДВАНЕ И РАЗРАБОТВАНЕ НА МЕТОДИ ЗА ПОВИШАВАНЕ НА КИБЕРСИГУРНОСТТА

АВТОРЕФЕРАТ
на
ДИСЕРТАЦИОНЕН ТРУД

за придобиване на образователна и научна степен
„ДОКТОР“

Професионално направление:
„Комуникационна и компютърна техника“
Докторска програма: „Автоматизирани системи за обработка на информация и управление“

Научен ръководител:
Полк. доц. д-р инж. Юлиян Иванов Цонев

Варна, 2021 г.

Дисертационният труд се състои от 172 страници.
Основен текст – 154 стр.
Брой на литературните източници – 116.
Брой на фигурите – 95.
Брой на таблиците – 10.
Брой на приложенията – 1.
Брой на публикациите по дисертацията – 6.

Защитата на дисертационния труд ще се състои на ..... от ..... ч. в зала ..... на ВВМУ „Н. Й. Вапцаров“.

Рецензиите, становищата на членовете на научното жури и авторефератът са публикувани в сайта на Училището, www.naval-acad.bg

Материалите по защитата са на разположение на интересуващите се в.....

Адрес: Варна, ул. „Васил Друмев“ №73

ВВМУ „НИКОЛА ЙОНКОВ ВАПЦАРОВ“
ФАКУЛТЕТ „ИНЖЕНЕРЕН“

Катедра „Информационни технологии“

инж. ДИМО БОЖИДАРОВ ДИМОВ

ИЗСЛЕДВАНЕ И РАЗРАБОТВАНЕ НА МЕТОДИ ЗА ПОВИШАВАНЕ НА КИБЕРСИГУРНОСТТА

АВТОРЕФЕРАТ
на
ДИСЕРТАЦИОНЕН ТРУД

за придобиване на образователна и научна степен
„ДОКТОР“

Професионално направление:
„Комуникационна и компютърна техника“
Докторска програма: „Автоматизирани системи за обработка на информация и управление“

Научен ръководител:
Полк. доц. д-р инж. Юлиян Иванов Цонев

Варна, 2021 г.

Дисертантът работи в Държавно предприятие „Ръководство на въздушното движение“ и е зачислен в задочна форма на обучение в катедра „Информационни технологии“ при факултет „Инженерен“ на ВВМУ „Н. Й. ВАПЦАРОВ”.

Изследванията са извършени във ВВМУ.

Дисертационният труд е насочен за защита от съвета на Факултет „Инженерен“ при ВВМУ „Н. Й. Вапцаров“ в съответствие с чл. 5, ал. 1 от ЗРАС.

Автор: Димо Божидаров Димов
Заглавие: Изследване и разработване на методи за повишаване на киберсигурността
Тираж: ..... броя.

СПИСЪК НА ИЗПОЛЗВАНИТЕ СЪКРАЩЕНИЯ

АД	Активна Директория
ЕС	Европейски Съюз
ОС	Операционна система
AD	Active Directory
DNS	Domain Name Services
ENISA	European Union Agency for Cybersecurity
GDPR	General Data Protection Regulation
GPO	Group Policy Object
GPP	Group Policy Preference
KDC	Key Distribution Center
MS	Microsoft
NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology
NTLM	NT Lan Manager
OS	Operating system
PS	PowerShell
PSO	Password Setting Object
SCCM	System Center Configuration Manager
SUS	Software Update Services
WSUS	Windows Server Update Services

I. ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

1. Актуалност на проблема

На 9 Юли 2016г. на среща на високо равнище във Варшава, съюзниците от НАТО вземат ключово решение официално да признаят киберпространството като домейн за осъществяване на операции, също както по суша, въздух, вода и в космоса. Позицията на НАТО по отношение на киберпространството е дефанзивна, но отправя ясен знак, че Алиансът укрепва своята киберотбрана във всички направления.

През последните няколко години са откраднати стотици милиони данни от кредитни карти, лични данни, отвличани са безпилотни летателни апарати, дори бяха поразени центрофуги за ядрено гориво. Атакуващият няма обособен социален профил. Той или тя може да бъде, както член на терористична групировка бореща се за своя кауза, така и обикновен зрелостник с упорит интерес в областта на информационните технологии. Общото във всяка сполучлива атака е експлоатацията на съществуваща уязвимост.

2. Проблем

В отговор на нарастващите кибератаки и престъпност е създадена и постоянно се обновява нормативна уредба (закони, правилници, разпоредби и др.), както са налице и организации, регулиращи процесите в киберпространството. В същото време липсват технически процедури, методи и способи за реализиране на изискуемите в съществуващата нормативна уредба изисквания и правила.

3. Цел и задачи на дисертационния труд

Целта на дисертационния труд е да се разработят методи за повишаване на киберсигурността на информационна инфраструктура чрез изграждане на хибридна система за прилагане на обновления и архитектура за управление на административни и привилегировани потребители.

За да бъде постигната поставената цел са набелязани следните **задачи**:

1) Да се направи анализ на съществуващи решения за управление на актуализации на Майкрософт базирани операционни системи.

2) Да се изследва времето за прилагане на обновления след тяхното публикуване в официални за това сървъри. На тази база да се изгради система за хибридно прилагане на обновления на операционната система без нарушаване на критични бизнес процеси в организацията;

3) Да се изследва зависимостта на времето, необходимо за разбиване на парола от нейната ентропия, дължина и сложност. Да се изгради архитектура за управление на административни и привилегировани потребители, управление на техните пароли, организиране на техните права и привилегии;

4) Да се изследва работоспособността на разработените методи. Чрез опитна постановка да бъдат изпълнени последователно серия от зловредни атаки върху лабораторен домейн преди и след прилагането на разработените методи. На база на експерименталните данни да се даде оценка на разработените методи относно степента на повишаване на киберсигурността.

4. Обект и предмет на дисертационния труд

В дисертационния труд, обект на изследване са Майкрософт базираните операционни системи и решения (предвид пазарния дял от 77,74% на десктоп операционните системи, следвани от macOS с 17,07% към Юли 2020): виртуализационни платформи, сървъри, работни станции (членове на домейн с активна директория), роли, инструменти и софтуерни продукти.

Предмет на изследване са системи за прилагане на обновления и централизирано управление на административни и привилегировани потребители.

5. Място на изследванията

Изследванията са извършени във ВВМУ.

6. Научна новост

Създадена е концепция на система за хибридна дистрибуция на обновления, която автоматично прилага новопубликувани актуализации на операционната система на пилотни групи и потребители. След изтичане на предварително дефиниран карантинен период, администратор ръчно позволява или забранява масовата дистрибуция и приложение на съответните обновления.

7. Практическа ценност

- Определени са характеристиките на пароли, които не могат да бъдат разбити в оперативен порядък, при предварително дефинирани условия;
- Предложена и създадена е архитектура за управление на административни и привилегировани потребители;
- Създаден е алгоритъм и на тази база скрипт за сравнение на

потребителите в базата на активната директория и потребителите в базата на Windows Server update Services;

- Създаден е алгоритъм и на тази база скрипт за поправка на агентите, които не докладват за статуса на работните станции в базата на Windows Server update Services;
- Създаден е лабораторен домейн за изследване работоспособността на хибридната система за прилагане на обновления и архитектурата за управление на административни и привилегировани потребители, позволяващ оценка на устойчивостта спрямо различни видове кибератаки.

8. Апробация на изследването

Основните резултати от проведените изследвания свързани с дисертационния труд са докладвани на следните международни научни конференции и форуми:

- CompSysTech - 18th International Conference, June 2017, Ruse, Bulgaria
- Constanta Maritime University 2-nd Black Sea Maritime CyberSecurity Conference, June 2018, Constanta, Romania
- SIELA Conference - 20th International Symposium on Electrical Apparatus and Technologies, June 2018, Burgas, Bulgaria
- EMENA-ISTL - 2nd international conference Europe Middle East & North Africa Information Systems and Technologies to support Learning, October 2018, Fez, Morocco
- DIGILIENCE 2020 - Information & Security, Oct, Varna, Bulgaria

II. СЪДЪРЖАНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

Увод

В увода накратко е представена актуалността на разглеждания проблем. Формулирани са основните насоки на работа и е обобщена кратка характеристика на структурата и съдържанието на отделните глави.

ПЪРВА ГЛАВА - Преглед на текущото състояние на предметната област и необходимостта от повишаване на киберсигурността

1.1. Преглед на настоящата нормативна уредба спрямо киберсигурността, сигурността на информацията и личните данни

В периода август 2018 – юли 2019 г. Националният екип за реагиране при инциденти регистрира непрекъснато усложняване на обстановката в

България по отношение на мрежовата и информационната сигурност. В интернет пространството ни за 2019 година са регистрирани 2851 сигнала, което е увеличение с 34% спрямо година по-рано.

1.1.1. Закон за киберсигурност

На 13 ноември 2018 г. в Държавен вестник е обнародван Законът за киберсигурност. Този закон се счита за първия подробен акт в българското законодателство в сферата на киберсигурността, в който са разписани разпоредбите в областта на мрежовата и информационната сигурност.

1.1.2. Наредба за минималните изисквания за мрежова и информационна сигурност

На 29 Юли 2019 влезе в сила новата Наредба за минималните изисквания за мрежова и информационна сигурност, която отменя досега съществуващата Наредба за общите изисквания за мрежова и информационна сигурност.

С Наредбата се определят минималните изисквания за мрежова и информационна сигурност, както и препоръчителни мерки, въвеждат се правила за извършване на проверките за съответствие с изискванията за мрежова и информационна сигурност, определя се редът за водене, съхраняване и достъп до регистъра на съществените услуги.

1.1.3. Общ регламент относно защитата на данните (GDPR)

С цел повишаване и гарантиране на съгласувано ниво на защита на физическите лица в целия Съюз и да се попречи на различията да възпрепятстват свободното движение на лични данни в рамките на вътрешния пазар, е необходим регламент, който да осигурява правна сигурност и прозрачност за икономическите оператори, включително за микро предприятията и малките и средни предприятия, и да предостави на физическите лица във всички държави членки еднакви по степен законно приложими права и задължения.

1.2. Международни стандарти свързани със сигурността на информацията

1.2.1. ISO/IEC 27001:2013

Международният ISO 27001:2013 е стандарт за управление на сигурността на информацията. Той поставя изисквания към Системите за управление на сигурността на информацията (СУСИ).

Системата за управление на сигурността на информацията е подход, който на първо място цели управление на поверителността, целостта и наличността на информацията в съответната организация.

Според стандартът, за да съхрани информацията си, организацията трябва да инициира следните стъпки:

- Да дефинира политика по информационната сигурност;
- Да идентифицира и оцени рисковете за сигурността;
- Да определи и внедри подходящи контроли за сигурността на информацията.

1.2.2. ISO/IEC 15408 Критерии за оценка на сигурността на информационните технологии

Стандартът ISO/IEC 15408 е по-популярен като „Общи критерии“ (Common Criteria, CC).

Общи критерии (ISO/ IEC 15408) е международен стандарт за оценка на сигурността на информацията. Този международно признат стандарт е създаден, за да оцени дали функциите за сигурност на дадена информационна система или информационен продукт са проектирани и изпълнени по подходящ начин, за да се противодейства достатъчно на заплахите. Понастоящем правителствата и големите корпорации в много европейски страни и Съединените американски щати предпочитат да закупуват сертифицирани продукти (ISO/IEC 15408), които отговарят на техните изисквания за възлагане на поръчки.

1.3. Европейски и световни агенции и институти, работещи в сферата на киберсигурността

1.3.1. Агенция на Европейския съюз за киберсигурност (European Union Agency for Cybersecurity – ENISA)

ENISA е експертен център в областта на кибернетичната сигурност в Европа. Агенцията помага на ЕС и страните членки да бъдат по-добре подготвени за предотвратяване, откриване и реакция на проблеми в сферата на информационната сигурност. Агенцията също така помага при изготвянето на политиката и законодателството на ЕС в областта на мрежовата и информационна сигурност.

1.3.2. Национален институт за стандарти и технологии (NIST)

Националният институт за стандарти и технологии (National Institute of Standards and Technology - NIST) е основан през 1901 г. и е част от американския департамент по търговия.

1.3.3. Институтът SANS

SANS е институт, предоставящ обучение за информационна сигурност и сертифициране в сферата на сигурността. Институтът разработва, поддържа и предоставя публично и безплатно най-голямата колекция от

изследователски документи за различни аспекти на информационната сигурност.

1.4. Кратък преглед на някои от популярните киберинциденти

1.4.1. Wannacry

В средата на Април 2017г. хакерската групировка “TheShadowBrokers” публично оповестяват експлойти и инструменти за пробив в Майкрософт базирани операционни системи. Те твърдят, че споменатите ресурси са разработени и активно използвани от Националната Агенция по Сигурност на САЩ и поради тази причина досега не са били публикувани, а умишлено пазени в тайна. Няколко часа след публикуваните от хакерската групировка новини, в официално изявление Майкрософт отричат тези уязвимости да са неизвестни. Шест от критичните уязвимости за отдалечено изпълнение на код са били адресирани чрез обновления и публикувани за безплатно изтегляне от потребителите на Майкрософт още през месец Март 2017г. Детайли за тези обновления са на разположение в бюлетин по сигурността „MS17-010“.

Въпреки че Майкрософт два месеца по-рано адресират уязвимостите, които хакерите използват, чрез ‘wannacry’ само за ден са били поразени стотици хиляди устройства. Броят им продължава да расте главоломно последващите дни.

1.4.2. NotPetya

На 27 Юни 2017г. стартира нова серия от кибератаки, първоначално в Украйна, а в последствие Русия и западна Европа докато епидемията не обхваща целия свят. В началото атаката изглежда като поредния ransomware целящ изнудване, но до 30 Юни става ясно, че това е диверсия и единствената цел на зловредния софтуер е да нанесе максимално щети без възможност за възстановяване на информацията.

Атаката стартира като обновление за популярна в Украйна счетоводна програма MeDoc. Подобна атака чрез софтуера MeDoc е извършена на 18 май 2017 г. с друг рансъмуер - XData. Експертите по киберсигурност са озадачени как на пръв поглед същият зловреден код използващ същите експлойти отново е в новините по цял свят, поразил стотици хиляди устройства. Инженерите, занимаващи се с изследване на зловреден код, установяват по-късно, че “EternalBlue” е просто още един от методите, който е използван от NotPetya за разпространение. Третият метод е кражба на акредитиви от потребителската станция.

Атаката разчита на вече познати уязвимости, както и вектори на атака, целящи кражба и преизползване на потребителски акредитиви.

1.4.3. Equifax

На 8 Септември 2017 Equifax признават, че са станали жертва на кибератака и в резултат са били откраднати огромно количество данни. Личните данни са на 143 милиона американски граждани – имена, рождени дати, номера на социални осигуровки, шофьорски книжки. Откраднати са и данните за 209000 кредитни карти. Обхватът и тежестта на този случай са безпрецедентни за времето си.

Основният фактор, който компанията твърди, че е довел до пробива е уязвимост в Apache Struts (CVE-2017-5638). Тази уязвимост позволява на атакуващия отдалечено да изпълнява команди.

Организацията "The Apache Software Foundation" открива потенциална уязвимост в продукта Apache Struts и изработва обновление, за да избегне експлоатация. Обновлението е публикувано на 7 Март 2017г. На 8 Март 2017г. Департаментът по национална сигурност на САЩ се свързва с Equifax, за да ги предупреди за уязвимостта и потенциалната опасност, ако не приложат обновлението свързано с Apache Struts. На 9 Март 2017г. организацията "The Apache Software Foundation" също се свързва с администраторите на Equifax, за да ги насърчат да приложат липсващото обновление.

Липсата на актуализация на Apache Struts е ключов фактор за провал. Анализът на атаката установява и допълнителни грешки в системата на Equifax, които са улеснили възникването на пробив - несигурен дизайн на мрежата поради липса на сегментиране, неадекватно криптиране на информация за личните данни на потребителите и неефективни механизми за откриване на пробиви.

1.4.4. Аварията в Белингам

На 10 юни 1999 г. тръбопровод, собственост на Olympic Pipeline Company, се пропуква и причинява изтичане на бензин в две малки реки в Белингам, Вашингтон. Бензинът се запалва, в резултат на което се получава експлозия, при която загиват трима души, ранени са осем души. Причинени са значителни имуществени и екологични щети след изпускането на около 1000 тона бензин.

Причината за аварията е комплексна. Външни повреди по тръбопровода, причинени по-рано от строителни дейности, неправилно настроени предпазни клапани за налягането, проблем при контролерите на SCADA системата, поради въвеждането на промени в компютърната система в контролния център от администратор на компанията.

В изследването на инцидента Маршал Ейбрамс и Джо Вейс обобщават, че ако бе приложена рамката от специалната публикация на NIST "800-53,

Recommended Security Controls for Federal Information Systems", внедрените оперативни, технически управленски и т.н. контроли са били в състояние да предотвратят аварията.

Изводи към Първа глава

1) В отговор на нарастващите кибератаки и престъпност е създадена и постоянно се обновява нормативна уредба (закони, правилници, разпоредби и др.), както са налице и организации, регулиращи процесите в киберпространството. В същото време липсват технически процедури, методи и способи за реализиране на изискуемите в съществуващата нормативна уредба изисквания и правила;

2) Анализираните кибератаки и инциденти доказват необходимостта за своевременното прилагане на обновления и управлението на потребителски акредитиви като критични необходимости в осигуряването на киберсигурността в информационните системи. Минимизирането на времето за прилагане на обновленията понижава риска от провеждането на успешни кибератаки и намалява възможностите за експлоатация на съществуващи уязвимости;

3) Минимизиране на времето за извършване на обновленията трябва да се извършва при отчитане на възможността за нарушаване на нормалната работоспособност на информационната система при прилагане на обновления без тяхното тестване за работоспособност и съвместимост.

ВТОРА ГЛАВА - Изследване, анализ и оценка на някои фактори за повишаване на киберсигурността

2.1. Системен и функционален анализ на системи за прилагане на обновления

2.1.1. Microsoft Windows Server Update Services (WSUS)

WSUS е роля, вградена функционалност в сървърните операционни системи на Майкрософт. Дава възможност на администраторите да прилагат, чрез графичен интерфейс (конзола) обновления свързани с продукти на Майкрософт на работни станции и сървъри в мрежата на организацията.

2.1.2. Microsoft System Center Configuration Manager (SCCM)

SCCM (Microsoft System Center Configuration Manager) представлява пакет от инструменти, необходими за администрация на средни и големи организации. Първоначалното внедряване изисква ресурси от гледна

точка на време, средства и умения на персонала. Продуктът позволява автоматизирането на дистрибуцията и приложението на обновленията, софтуер, драйвери и дори цели операционни системи по мрежата.

2.2. Изследване на екстремума на времето, необходимо за прилагане на обновления

За да бъдат избегнати прекъсвания на критични за организацията операции, в процеса за управление на обновленията се предлага добавянето на стъпки за тестване на обновлението в продуктивна среда чрез прилагане на обновлението на пилотна (тестова) група от устройства. По този начин, при докладването на неизправности или несъвместимости между новото обновление и устройството, масовото прилагане на обновлението може да се забави (за допълнителни тестове) или да бъде отложено до предоставяне на следваща версия или ревизия (фиг. 2.1).

Чрез допълнителните операции, цикълът на цялостно прилагане на новопубликувано обновление ще се състои от следните стъпки:

1) Системата синхронизира манифест за актуализациите и научава за наличието на ново обновление;
2) Системата изтегля новото обновление;
3) Системата одобрява за инсталация новото обновление за прилагане върху пилотна група от устройства;
4) Устройствата от пилотната група синхронизират със системата и научават за обновлението;
5) Устройствата от пилотната група изтеглят новото обновление от системата или от интернет;
6) Устройствата от пилотната група прилагат новото обновление;
7) Изчаква се определен период (карантинен срок) за проверка за несъвместимости или докладване на нередности:

   А) При открити или докладвани нередности се изследва първопричината. Докладва се на производителя на обновлението и/или проблематичното приложение или софтуерен продукт;

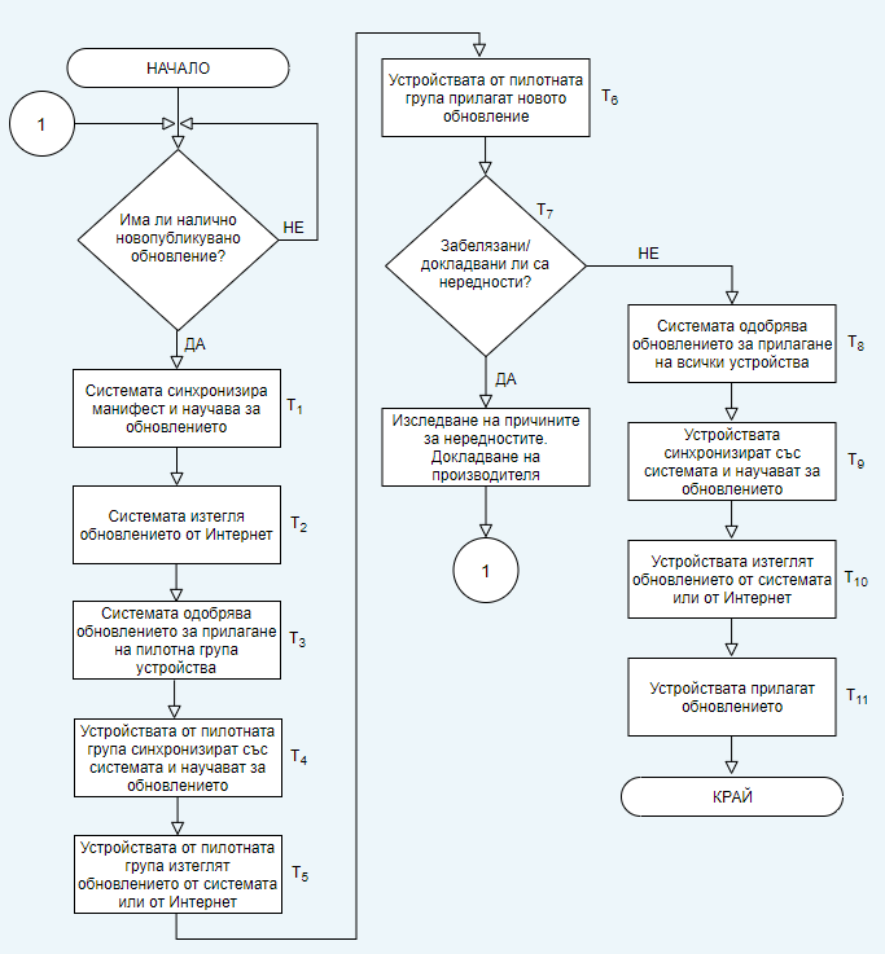
   Б) При липса на забелязани или докладвани нередности се продължава с прилагането на обновлението на останалите устройства в продуктивна среда;

8) Системата/администратор одобрява за инсталация новото обновление за прилагане на всички устройства;
9) Устройствата синхронизират данни със системата и научават за новото обновление, подходящо за инсталация;
10) Устройствата изтеглят новото обновление от системата или от

интернет;

11) Устройствата прилагат новото обновление.

Времето, необходимо за прилагане на едно обновление $T_{ОВПО}$ (общото време за прилагане на обновление) - от неговата поява до наличието на ресурса на крайното устройство - може да бъде зададено като сума от времената на отделните стъпки разгледани на фиг. 2.1.



Фиг. 2.1. Основни стъпки при прилагане на обновления с предварително прилагане върху пилотна група

Ако времето за изпълнение на стъпка 1 (T_1) е времето необходимо на

една организация да научи за наличието и синхронизира новопубликувано обновление, а изпълнението на стъпка 11 (T_{11}) е времето необходимо на крайното устройство (извън пилотната група) да приложи цялостно и безпроблемно новопубликуваното обновление, то може да се заключи, резултатът от формула (2.1) ще представи $T_{ОВПО}$.

$$T_{овпо}=\sum_{i=1}^{11} T_i \quad (2.1)$$

Ако се вземе предвид, че някои от стъпките могат да бъдат разделени на по-малки операции или да бъдат добавени допълнителни стъпки под формата на проверки, потвърждения, повторни опити и т.н., то времето необходимо за изпълнението на целия цикъл ще представлява сума от тези n на брой стъпки – формула (2.2)

$$T_{овпо}=\sum_{i=1}^{n} T_i \quad (2.2)$$

Постигане на минимално $T_{ОВПО}$ е възможно чрез автоматизация на някои или всички от стъпките, посочени във фиг. 2.5, чрез функционалностите на софтуерните продукти разгледани в т.2.1.

2.3. Анализ на NTLM и Kerberos протоколи за автентикация чрез SSPI модела в Microsoft операционни системи.

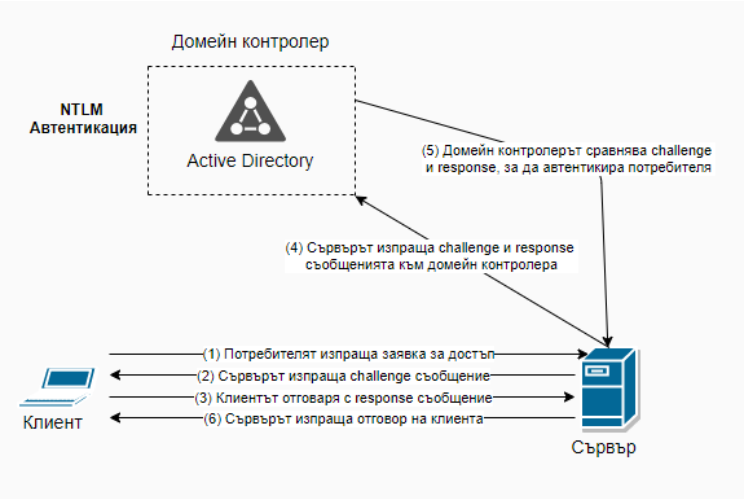
Security Support Provider Interface (SSPI) позволява на приложенията да използват различни модели за сигурност върху операционната система или по мрежата без промяна на интерфейса на системата за сигурност.

2.3.1. NTLM

Microsoft NTLM: името на протокола произлиза от съкращението NT LAN Manager. NTLM е протокол за автентикация по подразбиране в Windows NT 4.0.

NTLM е протокол за удостоверяване тип „предизвикателство-отговор“ (Challenge-Response – C/R). Стъпките на автентикация чрез NTLM са представени на фиг. 2.2.

Протоколът NTLM остава уязвим за атаката Pass-the-hash. Тази уязвимост е адресирана от обновление по сигурността публикувано от Майкрософт – MS-08-068. Например инструмент като Metasploit в много случаи може да се използва, за да получи акредитиви от едно устройство и да ги използва, за да получи контрол върху друго устройство.



Фиг. 2.2. Стъпки на автентикация чрез протокола NTLM

2.3.2. Kerberos

Протоколът се основава на криптиране чрез симетричен ключ като се изисква доверена трета страна. Възможно е да се използва и криптиране с публичен ключ по време на определени фази на автентикацията.

Протоколът Kerberos дефинира начинът, по който клиентите взаимодействат с мрежовите услуги за автентикация. Клиентите получават „билет“ (ticket) от дистрибуционния център за ключове (Kerberos Key Distribution Center – KDC) и предоставят тези ключове на сървърите, с които ще се осъществява връзка. Kerberos билетите представляват мрежовите акредитиви на клиентите в мрежата.

2.4. Фактори за постигане на силна парола

Силната парола е мярка за ефективността на паролата срещу отгатване (налучкване) или атака от типа “brute force”. Оценява се средния брой опити на атакуващия да посочи правилно паролата без да има пряк достъп до нея. Силата на паролата е функция на нейната дължина, сложност и непредсказуемост.

2.4.1. Анализ на сигурността на паролите с използване на ентропийна оценка

Ентропия е физична величина, която представлява мярка за безпорядъка на термодинамичните системи. Терминът „ентропия“ произхожда от гръцкия език: εν – вътре, τρέπω – пренасям. Ентропията е правопропорционална на логаритъма на броя на възможните

микросъстояния, съответстващи на дадено макросъстояние на системата.

2.4.2. Случайни (рандомизирани) пароли

За паролите, генерирани от процес, който избира на случаен принцип низ от символи с дължина, L, от набор от N възможни символа, броят на възможните пароли може да бъде намерен чрез повишаване на броя на символите до степен L, т.е. N^L. Увеличаването на L или N ще направи по-силна генерираната парола.

Силата на произволна парола, измерена от ентропията на информацията, е логаритъмът от втора степен от броя на възможните пароли, като се приема, че всеки символ в паролата е избран рандомизирано. Така ентропията на информацията за случайна парола H, се изчислява по формулата (2.3):

$$H = log_2 N^L = L\, log_2 N \qquad (2.3)$$

Където N е броят на възможните символи и L е броят на символите в паролата. H се измерва в битове.

2.4.3. Изследване на ентропията като фактор при генерирането на рандомизирани пароли

Чрез формула (2.3) и популярните символни набори – числа, малки/големи букви, ASCII символи, в таблица 2.1 е пресметната ентропията за 1 символ от съответния символен набор дефиниран в първата колона.

Табл. 2.1. Изчислена ентропия за различните символни групи низове

Символен набор	Брой символи	Ентропия за символ (bit)
Числа (0-9)	10	3.32192809489
Малки ИЛИ големи букви (a-z или A-Z)	26	4.70043971814
Малки ИЛИ големи букви И числа (a-z/A-Z, 0-9)	36	5.16992500144
Малки И големи букви (a-z, A-Z)	52	5.70043971814
Малки букви, големи букви и числа (a-z, A-Z, 0-9)	62	5.95419631039
Всички ASCII (printable) символи без шпация	94	6.55458885168
Всички Latin-1 символи	94	6.55458885168
Всички ASCII (printable) символи	95	6.56985560833
Всички допълнителни ASCII (printable) символи	218	7.76818432478

За да се изчисли дължината на паролата L, необходима за постигане на желаната ентропия H, с парола, съставена произволно от набор с N на брой символа, се използва формула (2.4):

$$L = \frac{\mathrm{H}}{log_2 \mathrm{N}} \qquad (2.4)$$

Като резултатът се закръгля към поредното цяло число.

2.4.4. Изследване на времето необходимо за разбиване на случайна парола

От данните изчислени в таблица 2.1 (чрез формула 2.3) в настоящата работата са изчислени (чрез формула 2.5) и консолидирани (табл. 2.2) резултатите при изследването на необходимото време за гарантирано изчисляване (разбиване) на случайна парола.

$$T = \frac{2^H}{V} \qquad (2.5)$$

Където T е времето за гарантирано разбиване на паролата. V е броят на подаваните предполагаеми комбинации (предположения) в секунда.

Табл. 2.2. Резултати от изчисляване на времето за разбиване на парола спрямо дължината, използваните символи, ентропията и броя опити за секунда

Ентропия H (битове)	Дължина на паролата L според ентропията за съответния набор от символи			Време за гарантирано отгатване на паролата чрез BruteForce – T			
				Брой опити в секунда - V			
	Малки букви	Малки, големи букви и цифри	Малки, големи букви, цифри и символи	1 000 000	$1*10^9$	$1*10^{11}$	$1*10^{12}$
40			6	13 дни	18 мин	11 сек	1.1 сек
42	9	7		51 дни	1.2 часа	44 сек	4.4 сек
44				6.7 мес	4.9 часа	2.9 мин	18 сек
46			7	2.2 год	20 часа	12 мин	1.2 мин
48	10	8		8.9 год	3.3 дни	47 мин	4.7 мин
50				36 год	13 дни	3.1часа	19 мин
52	11		8	143 год	1.7 мес	12.5часа	1.3 часа
54		9		571 год	6.8 мес	2.1 дни	5 часа
56	12			2300год	2.3 год	8.3 дни	20 часа
58				9100год	9 год	33 дни	3.3 дни
60		10	9	∞	37 год	4.4 мес	13 дни
62	13			∞	146 год	1.5 год	1.8 мес
64				∞	584 год	5.8 год	7 мес
66	14	11	10	∞	2300 год	23 год	2.3 год
68				∞	9400 год	94 год	9 год
70	15			∞	∞	374 год	37 год

В зелено са обозначени времената, които са над 10 000 години, необходими, за да се разбие дадена парола със съответните атрибути и брой опити за секунда. В жълто и оранжево са обозначени времената съответно 100-1000 години и 1-100 години. В червено и тъмно червено са обозначени комбинациите от атрибути, които генерират слаби пароли, за

чието разбиване е необходимо по-малко от една година.

2.5 Емпирично изследване на времето необходимо за пресмятане на NTLM хеш-стойност на парола според дължината и сложността й

Изчислението е осъществено чрез опитна постановка включваща физическо устройство със следните основни параметри:

- CPU: Intel Core i7-7700 CPU @ 3.60GHz;
- RAM: 16GB DDR4;
- HDD: 1TB SATA;
- GPU: Intel(R) HD Graphics 630 1.0 GB;
- NVIDIA GeForce GTX 1060 3GB;
- OS: Windows 10 (Build 10.0.18363.628);

Използван е инструментът Hashcat, като методът за атака срещу хеш-стойността е 'BruteForce'. Подбрани са 5 NTLM хеш суми на случайно генерирани пароли с дължина 8 символа (табл.2.3). Паролите съдържат различни комбинации от символи.

Табл. 2.3 Измерено време необходимо за изчисляване на NTLM хеш-стойности на 5 пароли с различни комбинации от 8 на брой символа

Парола №	Парола в явен текст	Изчислено време	Измерено време	% от всички комбинации	~опита/сек MH/s
Парола1	quomadse	16 сек	3 сек	18,33%	12643,5
Парола2	m7mrwafv	3:25 мин	2:58 мин	87,34%	13846
Парола3	fPvsQxRb	59:18 мин	31:10 мин	52,58%	15010,1
Парола4	vVna34ex	3:56 часа	2:08 часа	54,24%	15308,6
Парола5	J%1uQ4sB	4 дни 18 ч	1 ден 18 ч	36.71%	15857,6

Общото време необходимо за гарантирано разбиването на петте пароли според инструмента извършващ атаката е приблизително 4 дни 20 часа и 58мин. Времето, което отне на инструмента за да разбие петте пароли е приблизително 1 ден 20 часа и 41 мин.

2.6. Предложение за разработка на методи за повишаване на киберсигурността и дефиниране на изискванията към тях.

За да бъдат адресирани проблемите свързани с липса на актуализации или тяхното прибързано прилагане, както и слабостите и уязвимостите, които са налице при неправилно управление на административни и привилегировани потребители и техните пароли, в настоящата работа се предлага разработката на:

- система, която хибридно (полуавтоматизирано) да прилага обновления на операционните системи, като стремежът е насочен към

гарантиране липсата на неочакван отказ на критична услуга или процес в следствие на прилагането на актуализациите, както и минимизиране на времето необходимо за масова дистрибуция на съответното обновление;

- архитектура за управление на административни и привилегировани потребители, техните пароли и атрибути.

2.6.1. Изграждане на хибридна система за дистрибуция на обновления

Системата за дистрибуция на обновленията трябва да отговаря на следните изисквания и да бъде:

- Ефективна – системата трябва да постига поставените цели спрямо заложените резултати на разумна цена;
- Ефикасна – системата трябва да постига поставените цели спрямо заложените резултати по сигурен и безопасен начин;
- Надеждна – системата трябва навременно да адресира новопоявилите се обновления и да не внася допълнителни трудности за постигането на целите, поради фокусиране на администраторите върху самата нея;
- Интегрирана с АД – системата трябва да бъде интегрирана с активната директория в организацията;
- Гъвкава – системата трябва да може да адресира нуждите на организации от всякакъв тип, размер, структура, географско разположение и логическа мрежова топология;
- Опростена архитектура – архитектурата на системата трябва да бъде максимално опростена и ограничена от гледна точка на компоненти и модули изискващи допълнителен ресурс – енергиен, административен, финансов, за физическо разположение и т.н.
- Опростена администрация – администрацията на системата (първоначално разгърната и настроена) трябва да коства минимално време и усилие на администраторите;
- Автономна – трябва да се търси максимална степен на автономност. Системата трябва да може да изпълнява сама определени задачи и да взема определени решения при първоначално стриктно дефинирани правила и критерии;
- Полуавтоматизирана – системата трябва да може хибридно (автоматизирано и ръчно) да прилага обновления според предварително оценени, тестван и внедрени автоматизирани процеси;
- Консистентна – системата трябва да оперира с валидни данни, да предоставя акуратна и консистентна информация относно броя,

статуса, членството на устройствата в групите, както и приложените и липсващите обновления на съответното устройство.

2.6.2. Формулиране на изисквания към архитектурата за управление на административни и привилегировани потребители

В контекста на поставените цели и задачи в дисертационния труд и отчитайки добри индустриални практики и препоръки от Майкрософт, към архитектурата за управление на административни и привилегировани потребители са поставени следните изисквания:

- Структурата на обектите в активната директория да е организирана, прегледна и с унифицирана конвенция на именуване;
- Трябва да е възможно гранулярното предоставяне на права на потребители и администратори без значение от тяхното географско или йерархично разположение в организацията;
- Повишаване бързодействието на прилагането на груповите политики поради липсата на нужда от филтрация на потребителите според членство в групи;
- Предоставяне на възможност за гъвкаво управление на устройствата, използвани от привилегировани или административни потребители;
- Ограничаване на членството на потребителски обекти в локалните групи на устройствата;
- Ограничаване на членството на потребителски обекти в административни групи в активната директория;
- Прилагане на силна парола за всички потребители на домейна;
- Сегрегирано прилагане на силна парола за привилегировани и административни потребители на домейна;
- Рандомизиране на паролата на локалния администратор на устройствата в обхвата на активната директория;

Изводи към Втора глава

1) В работата са разгледани и сравнени решения за управление и прилагане на актуализации на операционната система и други софтуерни продукти;
2) Изследвано е общото време за успешно прилагане на обновления в продуктивни системи. Разгледани са факторите влияещи върху цикъла на прилагане на обновления;
3) Разгледани са основни протоколи за автентикация в Windows среда, техните характеристики и уязвимости;
4) Изследвани са различни характеристики и параметри на потребителската паролата. Изчислена е ентропията на паролата при

различни условия;
5) Емпирично е установено времето за разбиване на пароли при определена дължина и сложност;
6) В работата са формулирани изискванията към хибридната система за прилагане на обновления и архитектурата за управление на административни и привилегировани потребители.

ТРЕТА ГЛАВА - Разработване на методи за повишаване на киберсигурността

3.1. Хибридна система за дистрибуция на обновления

Основните елементи изграждащи Хибридната система за дистрибуция са: Windows Server Update Services (WSUS) инфраструктура, целеви (таргетни) групи, групови политики (GPO), класификация на обновленията, синхронизационен календар, автоматични одобрения, скрипт за автоматично търсене и поправяне на повредени агенти (фиг. 3.1).

3.1.1. Windows Server Update Services (WSUS) инфраструктура

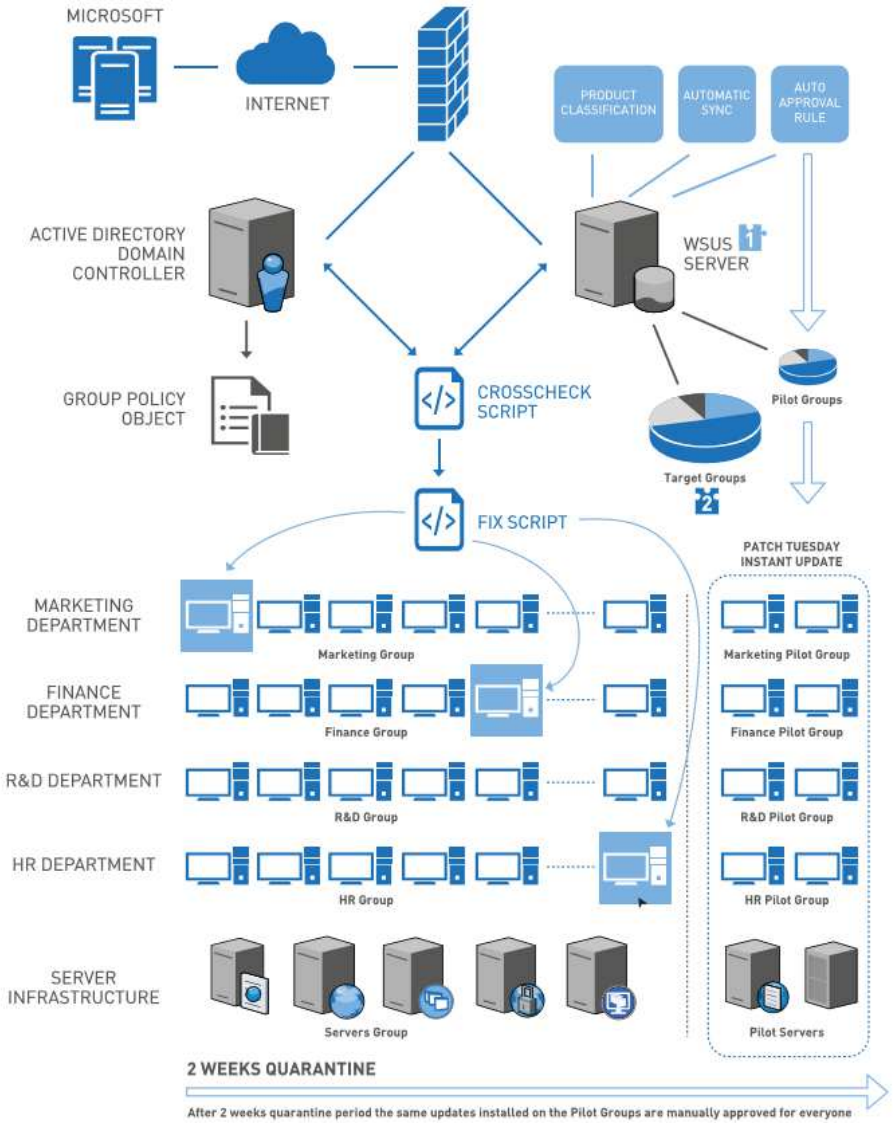
Ако се таргетират множество локации, в различни офиси, градове, държави трябва да се вземе предвид скоростта на връзката между локациите, броят устройства, ориентировъчното количество обновления и честотата на тяхното прилагане, и системните изисквания разгледани в т. 2.1.1. За да се опрости администрацията на подобна инфраструктура, се налага централизация на администрацията.

3.1.2. Дефиниране на целеви групи и техния обхват

WSUS дава възможност обновленията да се прилагат като се таргетират определени целеви (таргетни) групи. Тези групи не са групи от Активната директория (AD groups), а локални за WSUS групи.

Понеже основно изискване при изграждането на хибридната система за дистрибуция на обновленията е тя да бъде максимално автономна и консистентна – системата разчита на client-side метода.

Текущата система разчита на сегментация на база ролята на устройството (и потребителя на устройството) в организацията. Например устройствата, на които работят счетоводители и финансисти членуват в група “Finance Group”. Устройствата на потребителите от отдел „Маркетинг“ членуват в “Marketing Group” и т.н.



Фиг. 3.1. Хибридна система за дистрибуция на обновления

Хибридната система за дистрибуция на обновленията разчита на допълнителна сегментация, за да адресира потенциалната липса на тестови среди и възможността новоприложено обновление да доведе до отказ от услуга или деградация на качеството на някоя услуга.

Допълнителната сегментация се състои в добавянето на пилотни групи, отразяващи вече създадените целеви групи. Пилотните групи съдържат по няколко устройства (15%-20% от целевата група) и те първи автоматично ще получат новопостъпилите обновления.

При правилно структурирана и конфигурирана инфраструктура, новопубликуваните обновления могат да бъдат незабавно прилагани на пилотните групи. Времето за „карантина“ се счита за времето между инсталацията на обновленията на пилотните групи и прилагането на обновленията на устройствата в цялата организация.

Времето за карантина трябва да позволи на пилотните потребители да наблюдават и тестват изцяло поведението на приложенията и функционалностите по време на работа за потенциални нередности или отклонения от документираното очаквано поведение на системите.

3.1.3. Конфигуриране на групови политики

След като е установена и изградена сървърната инфраструктура от гледна точка на WSUS сървъри и групи е ред на клиентите (сървъри и работни станции) да бъдат насочени към съответния най-близък (географски или топографски) WSUS сървър и прилежащата целева група. Основна цел на настоящата система за дистрибуция на обновления е автономност и опростена администрация – настройките на клиентите са обезпечат чрез прилагане на групови политики на съответните обекти. Груповите политики специфицират определени настройки и стойности, необходими на клиента да се свърже, изтегли и при какви условия да инсталира съответното обновление, дали да направи рестарт след като инсталацията приключи.

3.1.4. Класификация на обновленията и избор на продукти. График на синхронизация

3.1.4.1. Класификация на обновленията

Чрез използването на функционалността за класификация, администраторите избират подходящите и необходими за организацията обновления, които да се изтеглят и синхронизират на WSUS инфраструктурата.

3.1.4.2. Избор на продукти

WSUS конзолата предоставя възможността да бъдат избрани продуктите, за които да бъдат синхронизирани актуализации. Администраторът може да направи детайлен избор на продуктите, за които Майкрософт осъществява поддръжка чрез WSUS.

3.1.4.3. График на синхронизация

Синхронизацията на обновленията с Microsoft Update може да се осъществи ръчно или автоматично. Ръчната синхронизация може да бъде използвана при нужда от форсиране на процеса. Препоръчително е използването на автоматичната синхронизация. Това ограничава нуждата от намеса на администратор, за да се изпълни операцията. Елиминира се варианта администраторът да забрави на изпълни синхронизацията, както и възможността да направи грешка при ежедневната администрация и конфигурация в конзолата.

3.1.5. Правила за автоматично одобряване на обновленията

Настройката на автоматичните правила има два основни аспекта: критерии за избор на обновленията, които се прилагат автоматично и целевите групи, за които се прилагат съответните правила.

В т.3.1.4. са определени чрез класификация на обновленията кои актуализации се синхронизират и изтеглят във WSUS средата, респективно и за кои продукти. На база тези дефиниции, са подбрани критериите за автоматично прилагане на правилата.

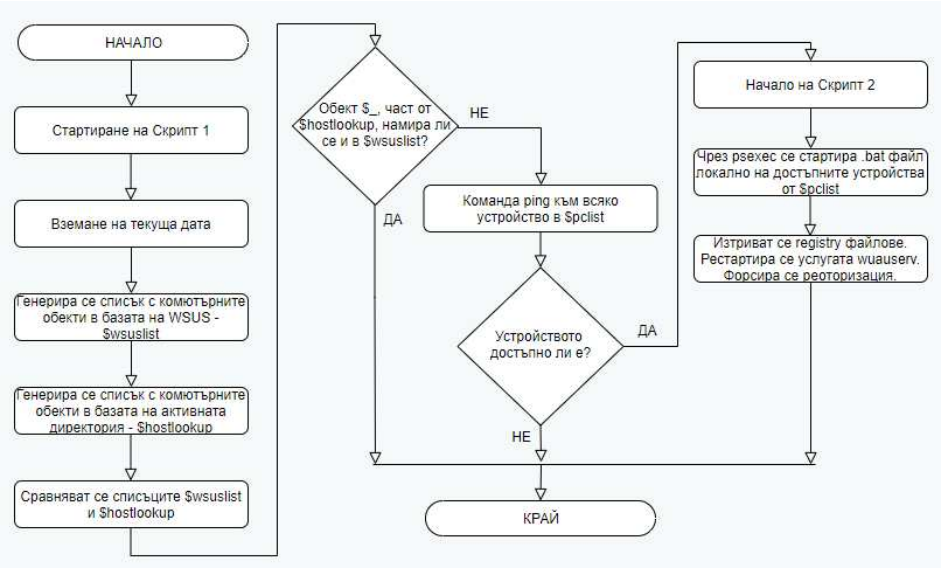
В т.3.1.2. са определени пилотни целеви групи съдържащи устройства от различни звена обезпечаващи критични за бизнеса процеси.

Чрез детайлната класификация на типа обновления, подборът на продуктите, които са част от основната софтуерна осигуровка (software baseline) на организацията и сегрегацията на пилотните целеви устройства се дава възможност да се дефинират правила за автоматично одобрение, които прецизно да предоставят желаните обновления на предварително набелязаните устройства.

3.1.6. Скриптове за автоматична поправка на повредени агенти

Важен аспект е постигането на максимална успеваемост при таргетирането на устройствата в обхвата на WSUS. Понякога някои от устройствата, макар и част от домейна, губят връзка със средата за дистрибуция и инсталация на обновленията.

Скрипт №1 прави сравнение между компютърните обекти в базата данни на активната директория и базата данни на WSUS. Съставя се списък с обектите съществуващи в АД, но липсващи в WSUS (фиг.3.2).
Обектите в списъка се таргетират един по един със скрипт №2, който изпълнява поредица от команди, целящи успешното стартиране на услугата и възстановяване на комуникацията с WSUS;



Фиг. 3.2. Блок схема на основните стъпки изпълнявани чрез скрипт 1 и скрипт 2

3.1.7. Обобщение на системата за хибридна дистрибуция на обновления

Максимизацията на автоматизацията и минимизирането на административните задачи ускоряват цялостно процеса на прилагане на обновленията. Прилагането на цялостната система осигурява заложените дефиниции в т. 2.6.1 и обезпечават безпроблемната работа на устройствата и критичните процеси и услуги въпреки регулярната дистрибуцията и приложение на обновления. Възникването на проблеми трябва да се адресира по време на карантинния период и потенциално афектираните устройства да бъдат само тези от пилотните групи.

3.2. Архитектура за управление на административни и привилегировани потребители

Внимателното планиране и изграждане на структурата на директорийните услуги - аранжирането на организационните единици, прилагането на груповите политики, групирането на привилегированите потребители и сегрегацията на последните спрямо необходимия им достъп до съответните ресурси ще доведе до наличието на зряла среда от гледна точка на архитектура и сигурност.

3.2.1. Аранжиране на организационните единици в активна директория

Според техническите спецификации на Майкрософт няма ограничение в броя на под-нивата на организационните единици, но от гледна точка на прегледност, администрация и улесняване на процеса при откриването на проблеми се препоръчват не повече от 10 под-нива. В конкретния случай под-нивата са 3. Те са достатъчни за групиране в следната йерархична структура:

- Ниво 1 – домейн, основно, най-ниско ниво. Прилагат се групови политики важащи за цялата организация.
- Ниво 2 – държава (град). В тази организационна единица е предвидено да бъдат разпределени крайните устройствата, потребителите, администраторите, сървърите и устройствата, които имат специален (различен от обичайния) достъп или ниво на привилегии;
- Ниво 3 – разпределение на различните обекти: потребители (обикновени и административни), устройства (работни станции или сървъри), групи, устройства със специален достъп.

3.2.2. Сегрегация на достъпа на местни администратори

Членството в Local Admin Group за устройствата трябва непременно да бъде контролирано и експлицитно дефинирано. Това може да бъде постигнато чрез прилагане на групова политика (в конкретния случай Group Policy Preference – GPP), която експлицитно дефинира кои потребители или групи да бъдат членове на Local Admin Group.

Груповата политика се прилага автоматично на всеки 90мин +/- 30 мин и е transparent (потребителя не разбира). Чрез този механизъм членството в групата остава фиксирано, както е дефинирано в груповата политика.

При наличната архитектура – организационни единици, потребители организирани в групи, потребителски и компютърни обекти намиращи се в определените за тях организационни единици е препоръчително добавянето на сходни групови политики определящи членството на потребители в следните чувствителни локални групи: Backup Operators, Event Log Readers, Power Users, Remote Desktop Users, System Management Users (и други локални групи според спецификите на съответната среда).

По този начин се добавят допълнителни ограничения и филтрация на достъп до услуги и ресурси, които иначе биха могли да се превърнат в цел и отправна точка за потенциална експлоатация.

3.2.3. Експлицитен контрол на членството в определени групи в активна директория

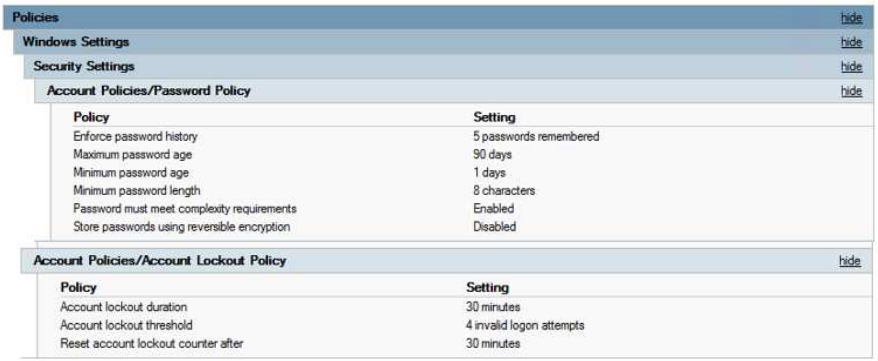
Отделна мярка добавяща допълнителен контрол и повишаваща нивото на сигурността при управлението на административните и привилегированите потребители (и групи) е прилагането на контрол върху членството в определени чувствителни групи. Тези групи могат да позволяват достъп до деликатни ресурси, да дават права за изпълнение на определени задачи, операции или използването на услуги. Такива групи могат да бъдат: Domain Admins, Entrerprise Admins, Schema Admins, O365 Admins, Account Operators (и други домейн групи според спецификите на съответната среда).

Груповата политика, адресираща Restricted Groups се състои от 2 основни части:

- Членове на групата – изброяват се поименно потребителите или други групи. След прилагане на политиката всички съществуващи членове на ограничената група, които не са изрично дефинирани в груповата политика се премахват автоматично;
- Членство на групата в други групи: изброяват се поименно групите, където ограничената група ще членува. След прилагане на политиката се осигурява членство на ограничената група в изрично дефинираните групи. Ако ограничената група членува и в други групи (освен изрично дефинираните), съответното членство се запазва.

3.2.4. Силна парола за всички потребители в домейна

На фиг. 3.3 е представена примерна политика за прилагане на правилата за силна парола в домейна. Освен правилата определящи атрибутите на паролата са дефинирани и стойности, които заключват потребителя при определен брой невалидни опити за автентикация.



Policies hide

Windows Settings hide

Security Settings hide

Account Policies/Password Policy hide

Policy	Setting
Enforce password history	5 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Account Policies/Account Lockout Policy hide

Policy	Setting
Account lockout duration	30 minutes
Account lockout threshold	4 invalid logon attempts
Reset account lockout counter after	30 minutes

Фиг. 3.3. Политика за прилагане на правила за силна парола

При така дефинирана групова политика, ако в рамките на 30 минути се направят 4 грешни опита – потребителят ще бъде заключен за 30 минути. Ако бъдат направени 3 неуспешни опита за автентикация в рамките на 30 минути потребителският акаунт няма да бъде заключен.

3.2.5. Сегментирана силна парола за привилегировани и административни потребители

Сегментираното прилагане на правила за силна парола на диверсифицирани групи в активната директория може да се извърши чрез използването на Fine-grained Password Policy и съответните правила - PSO (Password Setting Object).

Привилегированите потребители, администраторите и сервизните акаунти трябва да имат парола, която да бъде:

- по-дълга от тази на останалите потребители на домейна;
- трябва да се заменя по-често;
- заключва се след по-малък брой грешни опита за въвеждане;

3.3. Рандомизация на паролата на локалния администратор

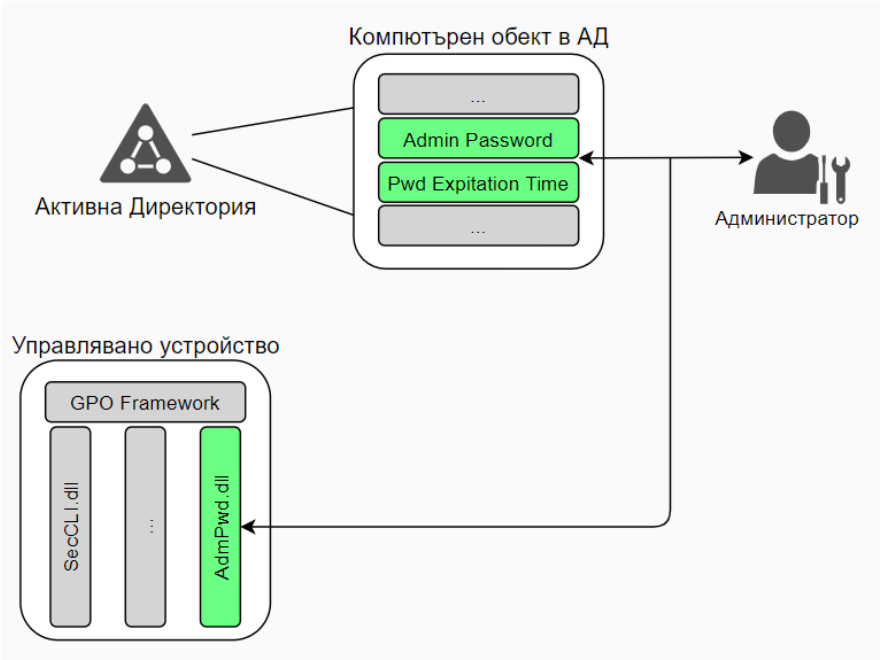
Използването на една и съща парола за локалния администраторски акаунт крие критични рискове за компрометирането на цялата организация. Прилагането на успешна атака върху един компютър или сървър и разкриването на паролата на локалния администратор би довела до шокиращи резултати за организацията.

LAPS (Local Administrator Password Solution) позволява централизираното съхранение на паролите (в базата на активната директория) и грануляраното раздаване на права на сътрудниците в организация за достъп до съответните пароли.

3.3.1. Минимални необходими компоненти

Минималните необходими компоненти (фиг. 3.4) на средата за безпроблемната работа на LAPS са:

- Агент – представлява Group Policy Client Side Extension (GPO CSE), който се инсталира посредством msi пакет;
- PowerShell модул;
- Активна директория – подсигурява отразяването на събития в Security Event Log-а на домейн контролера.



Фиг. 3.4. Основни компоненти на LAPS

След разширяването на схемата (Schema Extension), активната директория създава два нови конфиденциални атрибута за компютърните обекти - парола на вградения локален администратор и дата на изтичане на тази парола.

3.3.2. Основни процеси при работа на LAPS

Основните процеси при работата на LAPS са:

1) Проверка на давността на паролата на локалния администратор;
2) Смяна на паролата в случай на изтичане на давността или при форсирана смяна от оторизиран потребител (преди да е настъпило фактическото изтичане на периода на давност);
3) Докладва новата парола в активната директория и я съхранява в конфиденциален атрибут, който е част от компютърния обект в AD;
4) Докладва новата давност на паролата в активната директория и я съхранява в конфиденциален атрибут, който е част от компютърния обект в AD;
5) Паролата е достъпна и може да бъде прочетена от упълномощените потребители.

3.4. Обобщение

В Глава 3 на настоящата работа е представена разработката на два метода за повишаване на киберсигурността в една информационна инфраструктура. За да бъде постигнат синергитичен ефект от взаимно допълващите се продукти, инструменти, техники и подходи е необходимо методите да бъдат внедрени заедно и цялостно. По този начин може да се постигне така наречената "защита в дълбочина" (defense in depth), което може да попречи на една зловредна атака да бъде успешна дори и в случай, че някой от всички защитни механизми бъде компрометиран.

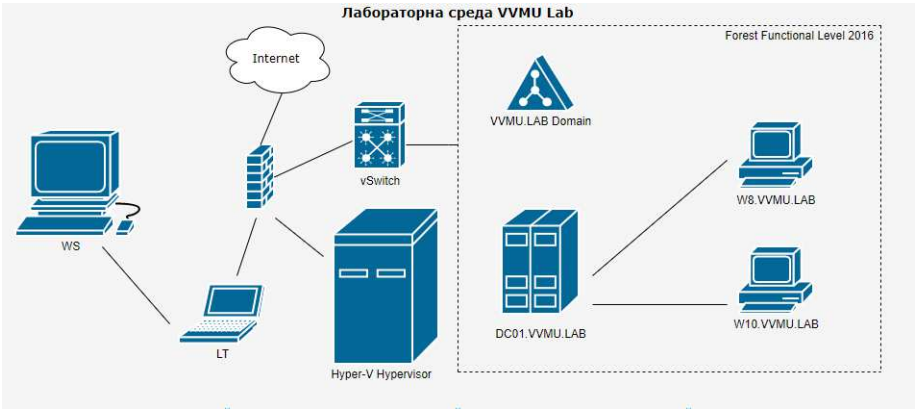
Изводи към Трета глава

1) Изградена е хибридна система за дистрибуция и прилагане на обновления според изискванията дефинирани в глава 2, т. 2.6.1;
2) Детайлно са представени характеристиките на внедрените компоненти, приложените процеси, изискванията и ограниченията на разработената система. Създадени са PowerShell скриптове за автоматизирана самопоправка на повредени агенти;
3) Изградена е архитектура за управление на административни и привилегировани потребители според изискванията дефинирани в глава 2, т. 2.6.2;
4) Детайлно са разгледани характеристиките на използваните компоненти и инструменти – организационни единици, групови политики, управление на приложените сегментации, сегрегации и експлицитни ограничения;
5) Направено е обобщение на извършените разработки.

ЧЕТВЪРТА ГЛАВА - Експериментални изследвания

4.1. Лабораторна среда за изследване на работоспособността на разработените методи за повишаване на киберсигурността

Изградената лабораторна среда (фиг. 4.1) се състои от Hypervisor Hyper-V, на който работят изолирано от хоста 3 виртуални машини свързани в общ VLAN чрез виртуален комутатор; работна станция (лаптоп) използван за изследване на снетите memory dump файлове и работна станция (стационарен компютър) с 2 видео карти, използван за BruteForce над откритите чрез различни инструменти и подходи NTLM хеш-стойности:



Фиг. 4.1. Логическа диаграма на ресурсите в лабораторна среда VVMU.lab

Основните устройства, част от опитната постановка са:

- Домейн контролер Windows Server Standard 2019 (DC01) с Forest Functional Level 2016 – част от лабораторен домейн;
- Работна станция Windows 10x64 (W10) – част от лабораторен домейн;
- Работна станция Windows 8.1x64 (W8) – част от лабораторен домейн;
- Работна станция (лаптоп) Windows 10x64 (LT);
- Работна станция (стационарен компютър) Windows 10x64 (WS).

4.2. Реализиране на сценарии преди прилагане на разработените методи за повишаване на киберсигурността

Реализирани са поредица от сценарии, изпълнени върху ресурси от лабораторната среда преди прилагането на предложените в Глава 3 методи за повишаване на киберсигурността. Заключение на база резултатите и кратък анализ от поведението на системите от лабораторната среда са обобщени в т. 4.2.6.

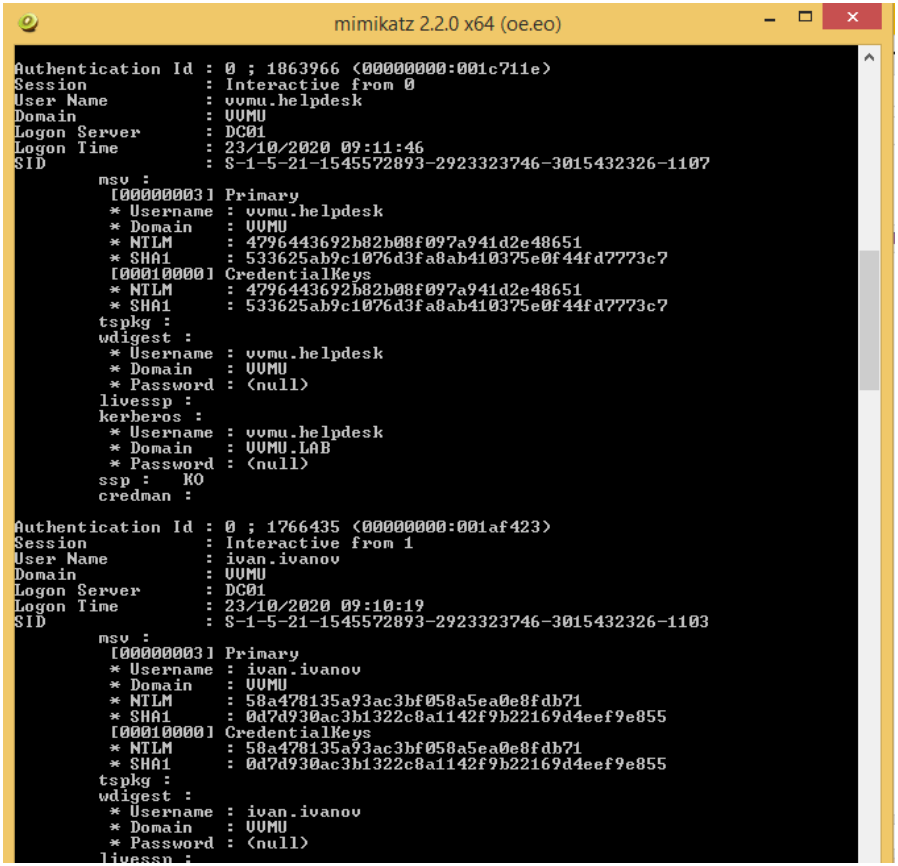
4.2.1.1 Извличане на акредитиви директно на работната станция чрез приложението mimikatz на работна станция W8

Чрез командата sekurlsa::logonPasswords се визуализират наличните данни за потребителите на съответната операционна система. В изходните данни са установени и детайлите за локалните потребители User и Administrator. Фокусът е насочен към наличните SIDs и съхранените хеш-стойности на паролите в NTLM:

vvmu.helpdesk: 4796443692B82B08F097A941D2E48651

ivan.ivanov: 58A478135A93AC3BF058A5EA0E8FDB71

user: 7D49CDDF4CB2E59B193412D3B7B6F17D
Administrator: 088B474DE1F6804CDEDA1F451A14CC33



Фиг. 4.2. Данни придобити чрез приложението mimikatz от работна станция W8

4.2.1.2. Извличане на акредитиви директно на работната станция чрез приложението mimikatz на работна станция W10

При първоначалния опит за стартиране на mimikatz на работна станция W10 вградените в операционната система механизми за превенция на злонамерен софтуер реагират и процесът е блокиран.

След експлицитно позволение на процеса, чрез задаване на изключение в Windows Security – Virus and Threat Protection – приложението се стартира успешно.

Подобно на стъпките в т.4.2.1.1. се изпълнява командата

privilege::debug за повишаване на привилегиите, следвана от командата за изчитане на детайлите в LSA: securlsa::logonPasswords

След изпълнението на последната команда стават видими хеш-стойностите на паролите на petar.petrov: 5318E6EE88980D18C499E7D37E79C926 и на локалния администратор на работна станция W10\Administrator: 088B474DE1F6804CDEDA1F451A14CC33

4.2.2. Извличане на NTLM хеш-стойности чрез инструменти за анализ на паметта (memory dump)

Използваният инструмент за целта на този сценарий е приложението DumpIT (memory forensics) на организацията Comae.

4.2.2.1. Извличане на NTLM хеш-стойности от работна станция W8 (чрез memory dump)

Създаденият .dmp файл съдържа в името си детайли за датата и точното време на снемане на memory dump-a.

Файлът бива преместен в отделна среда за последващ анализ и екстракция на наличните хеш-стойности. Анализът и опитът за екстракция се осъществят с помощта на приложението volatility – продукт на фондация с некомерсиална цел. Приложението се стартира в команден ред. Анализът на memory dump файла започва със следната команда:

```
volatility.exe -f W8-20201023-103725.dmp imageinfo
```

Следва опит за изчитане от паметта на адресацията (virtual offset) на регистрите (registry hives) на работна станция W8.

Използваната команда е следната:

```
volatility.exe -f W8-20201023-103725.dmp --profile=Win81U1x64 hivelist
```

Приложеният профил (Win81U1x64) е подходящ за наличния memory dump и адресите на съответните регистри са успешно изчетени:

- SYSTEM (0xffffc000eea28000);
- SAM (0xffffc000ef329000).

На фиг. 4.3. са представени изходните данни от изпълнението на командата за екстракция на наличните NTLM хеш-стойности от паметта на работна станция W8 според офсета (offset) на виртуалните адреси на кошерите SYSTEM и SAM. Използваната команда е следната:

```
volatility.exe -f W8-20201023-103725.dmp --profile=Win81U1x64 hashdump -y 0xffffc000eea28000 -s 0xffffc000ef329000
```

Фиг. 4.3. Успешно прочетени NTLM хеш-стойности от паметта на работна станция W8

Наличните NTLM хеш-стойности принадлежат на следните локални потребители: локалния администратор, гостът (guest) и потребителя USER, а техните NTLM хеш-стойности са съответно:
Administrator: 088b474de1f6804cdeda1f451a14cc33
Guest: 31d6cfe0d16ae931b73c59d7e0c089c0
Локален потребител User: 7d49cddf4cb2e59b193412d3b7b6f17d

4.2.2.2. Извличане на NTLM хеш-стойности от работна станция W10

Аналогични на стъпките извършени в предходната точка, процесът на извличане на хеш-стойности стартира с процедурата за снемане на memory dump от работна станция W10.

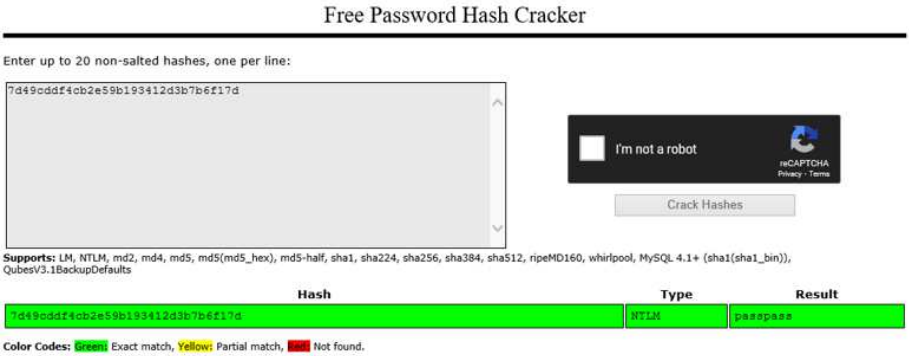
Профилът, използван за изчитането на позицията на регистрите в паметта е подходящ, но изтеглянето на хеш-стойностите е неуспешно поради несъвместимост между рандомизацията на паметта на операционната система и наличния профил.

4.2.3. Откриване на паролата в явен текст според придобитата NTLM хеш-стойност.

Следния сценарий цели откриването на паролата на база NTLM хеш-стойността чрез два различни подхода – търсене на съвпадение на вече изчислената NTLM хеш-стойност в популярни уебсайтове предлагащи тази услуга и чрез изчисляване на NTLM хеш-стойности до достигане на съвпадение (познат още като BruteForce).

4.2.3.1. Откриване на паролата в явен текст чрез популярни уеб сайтове

На фиг. 4.4. са приставени данните, които предоставя безплатен популярен сайт, които предлага услугата за проверка на NTLM хеш-стойности. Понеже паролата на локалния потребител User (от работна станция W8) е проста и сравнително кратка тя е известна на базата на crackstation.net.

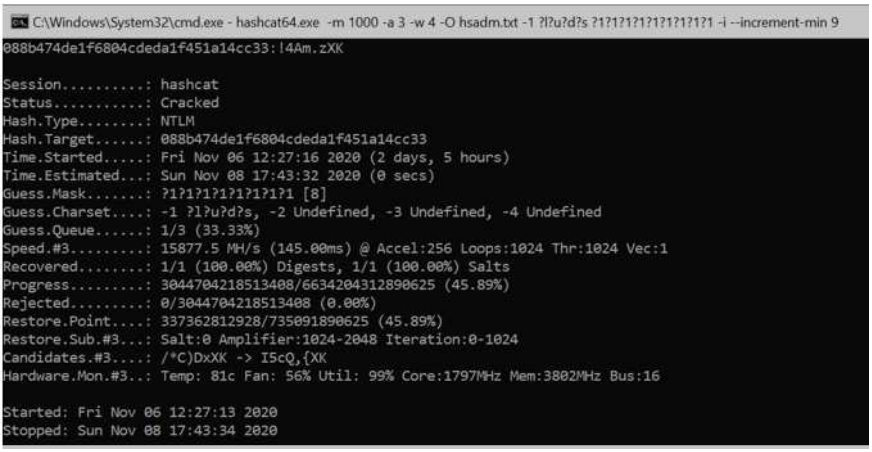


Фиг. 4.4. Проверка на NTLM хеш-стойността на паролата на локален потребите W8\User в популярен уебсайт в интернет

Паролата на потребител vvmu.helpdesk не е намерена с наличната NTLM хеш-стойност при претърсване в популярните онлайн бази с налични, изчислени предварително NTLM хеш суми.

4.2.3.2. Откриване на паролата в явен текст чрез инструменти за BruteForce.

Хеш-стойността е изчислен за 2 дни и 5 часа (фиг. 4.5) при достигане на 45,89% от потенциалните низови комбинации. Паролата на локалния администратор, съответстваща на NTLM хеш-стойността (088B474DE1F6804CDEDA1F451A14CC33), открита чрез Brute Force атака с помощта на инструмента Hashcat е "!4Am.zXK".



Фиг. 4.5. Разбиване на хеш-стойността на локалния администратор чрез BruteForce и инструмента hashcat

4.2.4. Отваряне на сесия чрез автентикация с хеш-стойност – атака от отипа PassTheHash

Следния сценарий има за цел преизползването на потребителски акредитиви (credentials reuse, в конкретния случай NTLM хеш-стойност) или изпълнението на атаката Pass-the-Hash (PtH). Атаката е изпълнена на работна станция W8 чрез приложението mimikatz.

Таргетираният потребител е този, чиято парола не беше открита в популярни сайтове, нито беше разбита с hashcat - vvmu.helpdesk.

Изпълнението на сценария се осъществява в следните стъпки:

1) Извеждат се детайли за текущия логнат потребител в операционната система ivan.ivanov;

2) Стартира се приложението mimikatz. Изпълнява се командата "privilege::debug", целяща повишаване на привилегиите до необходимите за изпълнението на следващата команда;

3) Изпълнява се командата: „sekurlsa::pth /user:vvmu.helpdesk /domain:vvmu.lab /ntlm: 4796443692B82B08F097A941D2E48651";

4) Подадената за автентикация NTLM хеш-стойност на потребителя vvmu.helpdesk срещу домейна vvmu.lab е приет, автентикацията е осъществена успешно;

5) Стартира се CMD сесия. Прави се проверка, в контекста на кой потребител е стартирана CMD сесията. Сесията е стартирана в контекста на vvmu.helpdesk.

4.2.5. Хоризонтално придвижване по мрежата

Следният сценарий е изпълнен от работна станция W8 към работна станция W10. За целта се стартира CMD конзола в контекста на потребителя ivan.ivanov. Потребителят стартира процеса Explorer.

За автентикация се използват потребителско име "W10\Administrator" и паролата на локалния администратор – Administrator, отгатната успешно чрез BruteForce атака в т. 4.2.3.2. върху NTLM хеш-стойността на паролата придобит в т. 4.2.1.1. Автентикацията се извършва локално срещу работна станция W10.

4.2.6. Обобщени резултати от приложените сценарии

След опит за извличане на акредитиви (чрез приложението mimikatz и изчитането на memory dump) от двете работни станции (членове на домейна), са открити артефакти, свързани с локални потребители и потребители от домейна, техните SIDs, хеш-стойности на паролите. Детайлите са представени в таблица 4.2.

Табл. 4.2. Артефакти открити при изпълнение на сценарии по т 4.2.

Потреб. име	Host	Член на домейна	Открит NTLM	Парола (открита чрез)
vvmu.helpdesk	W8	ДА	4796443692B82B08 F097A941D2E48651	-
ivan.ivanov	W8	ДА	58A478135A93AC3B F058A5EA0E8FDB71	**Password123** (crackstation.net)
petar.petrov	W10	ДА	5318E6EE88980D18 C499E7D37E79C926	**Initial123** (Hashes.com)
Administrator	W8/W10	НЕ	088B474DE1F6804C DEDA1F451A14CC33	**!4Am.zXK** (BruteForce атака)
User	W8	НЕ	7d49cddf4cb2e59b 193412d3b7b6f17d	**passpass** (crackstation.net)

Три NTLM хеш-стойности: на двама потребители от домейна (ivan.ivanov и petar.petrov) и потребителя User на работна станция W8 са успешно открити в популярни сайтове предлагащи безплатна проверка за съвпадения на NTLM хеш-стойности и символни низове.

Хеш-стойностите на паролите на локалния администратор на работна станция W8/W10 и на потребителя на домейна vvmu.helpdek са подложени на BruteForce атака чрез инструмента hashcat.

Времето необходимо за разбиване на хеш-стойността на локалния администратор е 2 дни и 5 часа.

Разбиването на хеш-стойността на паролата на потребител vvmu.helpdek не даде положителен резултат. Инструментът използван за BruteForce изчисли всички възможни 8 символни комбинации от сложни пароли за 4 дни и 17 часа без да има налично съвпадение. Времетраенето за разбиването на парола с дължина 9 символа състояща се от малки, големи букви, цифри и специални знаци (с наличните ресурси в лабораторната среда) е 1 година и 101 дни.

4.3. Прилагане на разработените методи за повишаване на киберсигурността

4.3.1. Изграждане и настройка на WSUS инфраструктура

Изграждането на WSUS инфраструктурата следва последователността описана детайлно в Глава 3, точка 3.1:

1) Инсталирана е Windows Server Update services ролята на сървър DC01;
2) Дефинирана е една целева група (LabGroup) за нуждите на лаборантите тестове;
3) Конфигурирана е групова политика;

4) Подбрана е класификация на продуктите, избрани са продуктите, за които ще има на разположение обновления;
5) Създаден е график за синхронизация;
6) Създадени са правила за автоматично одобрение на обновленията;
7) Приложени са всички актуални обновления на устройствата в лабораторната среда (членуващи в домейн VVMU.LAB);

Приложени са всички налични критични обновления, както и актуализациите свързани със сигурността на операционната система. Устройствата са рестартирани, за да се финализира цялостно приложението на обновленията.

4.3.2. Сегрегация на достъпа на местни администратори

Създадена е групова политика, която управлява експлицитното членство на локалните администратори. Политиката премахва всякакви потребители и/или групи (на устройствата, на които е приложена). Груповата политика налага следните потребители в групата на локалните администратори:

- Вградения локален администратор VVMULocal Admin;
- потребителя от домейн VVMU – vvmu.helpdesk;
- Global Security групата от домейн VVMU – Domain Admins.

4.3.3. Прилагане на експлицитен контрол на членството в определени групи в активната директория

Създадена е групова политика, която експлицитно налага членовете на чувствителни групи от домейна VVMU.LAB.

4.3.4 Прилагане на силна парола за всички потребители в домейна

Коригирана е “Default Domain” политиката (приложена за всички потребители на домейна) за налагане на правила за парола. Добавени са правила за заключване на потребителския акаунт за 30 минути след въвеждане на 3 грешни пароли в рамките на 30 минути. Потребителският акаунт следва да се отключи автоматично 30 минути след последния неуспешен опит за автентикация срещу домейна.

4.3.5. Сегментирана силна парола за привилегировани и административни потребители

Създадени са правила за управление на паролите на определени административни групи чрез Password Setting Object. Правилата са по-рестриктивни спрямо груповата политика приложена в т. 4.3.4. и целят обезпечаване на сигурността на административните акаунти.

4.3.6. Рандомизация на паролата на локалния администратор

Внедряването на софтуерния продукт LAPS (Local Admin Password Solution) изисква схемата на гората (domain forest) да бъде разширена с няколко допълнителни атрибута.

Създадена е групова политика, която определя детайли като дължината и сложността на паролата, както и името на вградения локален администратор (.500). Груповата политика е приложена на целия домейн.

На всички обекти, които са управлявани чрез LAPS е инсталирана клиентската част от софтуерния пакет на LAPS.

4.4. Реализиране на сценарии след прилагане на разработените медоди за повишаване на киберсигурността

4.4.1. Извличане на акредитиви директно на работната станция чрез приложението mimikatz

4.4.1.1. Извличане на акредитиви директно на работната станция чрез приложението mimikatz на работна станция W8

При навигиране до ресурсите за стартиране на софтуерния продукт mimikatz се визуализира прозорец на Windows Defender. Windows Defender информира за наличието на зловреден софтуер, който е премахнат.

Въпреки опита за премахване на mimikatz от контейнера за карантина и добавянето на приложението като позволено, операционната система и в частност Windows Defender не позволи да бъде стартирано.

4.4.1.2. Извличане на акредитиви директно на работната станция чрез приложението mimikatz на работна станция W10

По аналогичен случай с точка 4.2.1.2. и точка 4.4.1.1. приложението mimikatz не е стартирано успешно. В сценария от т. 4.2.1.2. приложението е добавено като изключение след засичането от Microsoft Defender.

Въпреки изключения Firewall и изричното позволение за стартиране на mimikatz, операционната система не позволява стартиране, а блокира и карантинира приложението.

4.4.2. Извличане на NTLM хеш-стойности чрез инструменти за анализ на паметта (memory dump)

4.4.2.1. Извличане на NTLM хеш-стойности от работна станция W8 (чрез memory dump)

Memory dump файловете са генерирани успешно за 26 секунди.

Стартира се изчитане на адресите на регистрите от memory dump

файла чрез следната команда, като този път използвания профил е различен от профилът приложен в т. 4.2.2.1, а именно Win8SP1x64_18340.

Виртуалните и физическите адреси на регистрите са успешно изчетени и визуализирани.

Следва опит за екстракция на хеш-стойностите според офсета (offset) на виртуалните адреси на кошерите SYSTEM (0xffffc001b9e28000) и SAM (0xffffc001bb140000). Използваната команда е:

volatility.exe -f W8-20201023-103725.dmp --profile= Win8SP1x64_18340 hashdump -y 0xffffc001b9e28000 -s 0xffffc001bb140000

Успешно са визуализирани NTLM хеш-стойностите на паролите на локалния администратор на работна станция W8 и потребителя Guest.

VVMULocalAdmin:C3C408BD0B3BB8696657B2A302C2B58D
Guest : 31D6CFE0D16AE931B73C59D7E0C089C0

4.4.2.2. Извличане на NTLM хеш-стойности от работна станция W10 (чрез memory dump)

След рестартиране на операционната система е направен втори, успешен опит за изпълнението на процедурата по снемане на memory dump от работна станция W10. Времето необходимо за генериране на файловете е 40 секунди.

Профилът използван за изчитането на позицията на регистрите в паметта е подходящ, но изтеглянето на NTLM хеш-стойностите е неуспешно поради несъвместимост между рандомизацията на паметта на операционната система и наличния профил.

Извличането на NTLM хеш-стойностите от работна станция W10 чрез memory dump е неуспешно.

4.4.3. Откриване на паролата в явен текст според придобитата NTLM хеш-стойност

4.4.3.1. Откриване на паролата в явен текст чрез популярни уеб сайтове

Единствената NTLM хеш-стойност, която е установена е тази на локалния администратор на работна станция W8.

Паролата съответстваща на NTLM хеш-стойността не е открита при проверка в популярните търсачки и бази съдържащи предварително преизчислени хеш суми на случайни низове.

4.4.3.2. Откриване на паролата в явен текст чрез инструменти за BruteForce

При направения опит за отгатване на паролата според наличната

NTLM хеш-стойност, приложението hashcat изчисли предполагаемо време от 1 година и 81 дни за откриване на съвпадение в целия обхват от възможни комбинации от низове съдържащи целия набор от малки букви, големи букви, цифри и специални символи за само 9 символа дължина на паролата. След прилагане на LAPS, дължината на паролата на локалния администратор е 16 символа.

4.4.4. Отваряне на сесия чрез автентикация с NTLM хеш-стойност – атака от типа PassTheHash

След прилагането на методите предложени в Глава 3, приложението mimikatz, чрез което беше осъществена атаката PassTheHash в т. 4.2.4. вече не може да бъде стартирано и сценарият не може да бъде репликиран успешно заради приложените актуализации свързани със сигурността на операционната система.

4.4.5. Хоризонтално придвижване по мрежата

Поради внедрената рандомизация на паролата на локалния администратор на устройствата, членуващи в домейна, всяко едно устройството попаднало под обхвата на LAPS има различна парола на вградения локален администратор.

4.4.6. Обобщени резултати от приложените сценарии след прилагането на методите разработени в Глава 3

След прилагането на разработените в Глава 3 методи, успешно беше изпълнено изтеглянето на NTLM хеш-стойността на паролата на локалния администратор от паметта на работна станция W8. Благодарение на рандомизацията на паролите на локалните администратори, не е възможно преизползването на NTLM хеш-стойността срещу други ресурси от лабораторния домейн освен работна станция W8. Отгатването на паролата с наличната процесорна мощност в лабораторната среда би отнело повече от 1,7 трилиона години.

Според резултатите получени от изпълнените сценарии, след прилагането на методите разработени в Глава 3, може да се заключи, че разработените и приложени методи ефикасно повишават защитата и нивото на киберсигурност до степен, средата да бъде устойчива на изпълнените чрез опитната постановка атаки, както и на атаки със сходни вектори на атака.

Изводи към Четвърта глава

1) Създадена е лабораторна среда – виртуализационно устройство, на което се помещават: домейн контролер, работни станции, виртуален комутатор; лаптоп, работна станция. В лабораторната среда е

създаден домейн, работните станции са пълноправни членове на домейна. Всички операционни системи са в срок на поддръжка от производителя (Windows server 2019, Windows 10, Windows 8.1. Всички използвани софтуерни продукти и инструменти са безплатни или в тестов период на експлоатация.

2) Изпълнени са няколко сценария на успешни атаки чрез различни инструменти и подходи към различни ресурси от лабораторната среда. Направен е обстоятелствен анализ на резултатите от изпълнените сценарии. Снети са екранни снимки.
3) В лабораторната среда са приложени хибридната система за прилагане на обновления и архитектурата за управление на административни и привилегировани потребители и е повторен опитът за изпълнение на същите атаки към ресурси от виртуалния домейн. Представени са детайли, разяснения и екранни снимки към резултатите от неуспешното изпълнение на атаките към ресурсите на лабораторния домейн.
4) Направено е обобщение на резултатите от изпълнените сценарии след прилагането на методите за повишаване на киберсигурността. Получените резултати доказват, че разработените методи повишават защитата и нивото на киберсигурността.

ЗАКЛЮЧЕНИЕ

След дефиниране на целта и задачите, които трябва да се изпълнят за нейното постигане, за осъществяването на настоящия дисертационен труд са извършени дейности, в резултат от изпълнението, на които е:

- направен системен и функционален анализ на среди за управление на прилагането на актуализации:
  - Microsoft Windows Server Update Services (WSUS);
  - Microsoft Systems Center Configuration Manager (SCCM)
- създаден модел за оценка на екстремума на времето необходимо за прилагане на актуализации;
- направен преглед и анализ на действието протоколи за автентикация:
  - NTLM;
  - Kerberos;
- направен анализ на силата на паролата според дължината, сложността и ентропията ѝ;
- направен е нализ на сигурността на паролите с използване на ентропийна оценка;
- изчислено е времето на гарантирано разбиване на парола според

различни нейни характеристики;

- емпирично е получено времето за гарантирано разбиване на NTLM хеш-стойност според различни характеристики на паролата;
- дефинирани са изисквания за разработване на:
  - хибридна система за дистрибуция на обновления;
  - модел на архитектура за управление на административни и привилегировани потребители;
- създадени са:
  - хибридна система за дистрибуция на обновления;
  - модел на архитектура за управление на административни и привилегировани потребители;
  - скрипт за търсене на повредени WSUS агенти;
  - скрипт за поправка на повредени WSUS агенти;
  - опитна постановка – лабораторен домейн с различни по вид ресурси;
- извършени са серия от експериментални изследвания върху опитната постановка – зловредни атаки, преди и след внедряването на разработените методи.

Научно-приложни приноси

1) Създадена е концепция на система за хибридна дистрибуция на обновления, която автоматично прилага новопубликувани актуализации на операционната система на пилотни групи и потребители. След изтичане на предварително дефиниран карантинен период, администратор ръчно позволява или забранява масовата дистрибуция и приложение на съответните обновления.

Приложни приноси

1) Определени са характеристиките на пароли, които не могат да бъдат разбити в оперативен порядък, при предварително дефинирани условия;
2) Предложена и създадена е архитектура за управление на административни и привилегировани потребители.
3) Създаден е алгоритъм и на тази база скрипт за сравнение на потребителите в базата на активната директория и потребителите в базата на Windows Server update Services;
4) Създаден е алгоритъм и на тази база скрипт за поправка на агентите, които не докладват за статуса на работните станции в базата на Windows Server update Services;

5) Създаден е лабораторен домейн за изследване работоспособността на хибридната система за прилагане на обновления и архитектурата за управление на административни и привилегировани потребители, позволяващ оценка на устойчивостта спрямо различни видове кибератаки.

Списък на публикации по темата на дисертационния труд

1. Dimov D., Tsonev Y., "Pass-the-Hash: One of the Most Prevalent Yet Underrated Attacks for Credentials Theft and Reuse", CompSysTech 18th International Conference, June 2017, Ruse, Bulgaria, DOI: 10.1145/3134302.3134338;

2. Dimov D., Tsonev Y., "Adaptive patching strategy", Constanta Maritime University Annals 27th issue, January 2018, Constanta, Romania, 10.38130/cmu.2067.100/42/28;

3. Dimov D., Tsonev Y., "Semi-automated system updates deployment solution assuring zero business disruption", SIELA Conference: 20th International Symposium on Electrical Apparatus and Technologies, June 2018, Burgas, Bulgaria, 10.1109/SIELA.2018.8447135;

4. Dimov D., Tsonev Y., "Result Oriented Time Correlation Between Security and Risk Assessments, and Individual Environment Compliance Framework", Proceedings of EMENA-ISTL: Information Systems and Technologies to Support Learning, Jan 2019, 10.1007/978-3-030-03577-8_42;

5. Dimov D., Tsonev Y., "Observing, Measuring and Collecting HDD Performance Metrics on a Physical Machine During Ransomware Attack", ISIJ 47: DIGILIENCE 2020, Information & Security: An International Journal 47, no. 3 (2020): 317-327, January 2020, DOI: 10.11610/isij.4723;

6. Dimov D, Tsonev Y., "Measuring and Comparing HDD Vital Signs During Ransomware Encryption" (под печат).